пания *Groteck* – издатель с 1993 года

СИСТЕМЫ БЕЗОПАСНОСТИ

циалистов

S&S

апрель – май 2021 № 2 (158)

ME!

ГОЛОВОЙ?

НИЕ! СПЕЦИАЛЬНЫЙ ЖУРНАЛ!

ать руководителю, ответственному за безопасность организации, или начальнику технического отдела!

BEWARD TFR80-210T1

Встроенное распознавание лиц

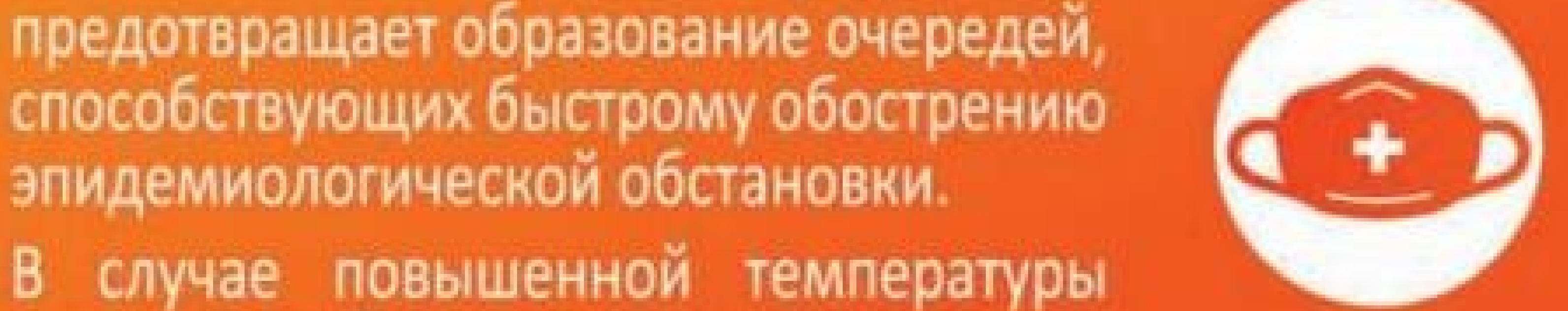
IP-терминал разработан с применением технологии распознавания лиц **BEWARD Bi-Scan**, которая позволяет сделать процесс распознавания исключительно точным и минимизировать время распознавания до 0,5 с, несмотря на работу в большой базе на 24 тыс. лиц. Функционал распознавания лиц работает автономно и не зависит от подключения к локальной сети или доступа в Интернет.



BEWARD Bi-Scan исключает возможность прохода по фотографии (в том числе с экрана мобильных устройств)

Бесконтактное измерение температуры

Процесс проверки температуры занимает всего 0,3 секунды, что предотвращает образование очередей, способствующих быстрому обострению эпидемиологической обстановки.



В случае повышенной температуры тела доступ будет запрещен, оператору системы придёт уведомление и будет проиграно тревожное сообщение через встроенный динамик. Также терминал способен определять, надета ли у проверяемого маска на лицо. Перечисленные функции позволяют избежать покупки тепловизионных систем, значительно превосходящих такие терминалы по цене.



Особенности:

- Диагональ экрана 8", светодиодная подсветка
- База распознавания на 24 тыс. лиц
- Точность ИК датчика температуры до ± 0,2°C
- Высокочувствительный сенсор 1/2,8" SONY Starvis
- Разрешение 1920x1080 пк @ 25 кадр/с
- Подключение RFID-считывателя по WIEGAND
- Работа с контроллером СКУД по WIEGAND-выходу
- Отправка кода карты при распознавании лица
- Многофакторная настраиваемая идентификация
- Широкая линейка аксессуаров

www.beward.ru

Компания *Groteck* – издатель с 1993 года

СИСТЕМЫ БЕЗОПАСНОСТИ

Журнал для руководителей и специалистов в области безопасности



апрель – май 2021
№ 2 (158)



В ЦИФРУ С ГОЛОВОЙ?

ВНИМАНИЕ! СПЕЦИАЛЬНЫЙ ЖУРНАЛ!
Передать руководителю, ответственному за безопасность вашей организации, или начальнику технического отдела!

www.secuteck.ru

Это безумный, безумный, безумный, безумный мир


Андрей Мирошкин,
генеральный директор
компании "Гротек"


Наталья Матлахова,
руководитель проекта
"Системы безопасности"
компании "Гротек"


Марина Бойко,
главный редактор проекта
"Системы безопасности"
компании "Гротек"

Цифровизация мира идет вперед семимильными шагами. Дроны доставляют почту в отдаленные уголки Великобритании, приобрести любой товар там, где есть Интернет, можно, не вставая с дивана, смартфоны, банкоматы и видеокамеры "узнают" лица...

Системы безопасности успешно противостоят новым угрозам, таким например, как пандемия коронавируса. В рекордные сроки были разработаны новые приборы для термометрии, технологии для распознавания по части лица и т.д.

В ритейле "новая нормальность" подтолкнула e-commerce и способствовала развитию уже применяемых ранее технологий, например биометрии и нейросетевой аналитики. В этом номере немало материалов, посвященных данной теме.

Мы рассказываем также об изменении законодательных требований в области охранной и пожарной сигнализаций и пожарной безопасности, советуем, как правильно выбрать биометрическую систему, делимся секретами производителей систем видеонаблюдения, прогнозируем будущее с использованием технологий виртуальной и дополненной реальности. Особое место занимают мнения экспертов об объективах для видеонаблюдения и рынке охранных услуг.

Безопасность мест с массовым пребыванием людей будет одной из ключевых тем следующего номера. Однако в связи с трагедией в Казани мы не могли оставить этот вопрос без внимания. О необходимости изменения парадигмы безопасности, выведения на новый уровень проектных работ, повышения эффективности защиты образовательных учреждений читайте в разделе "Комплексная безопасность".

Профессиональному сообществу потребуется еще много усилий, чтобы не только вывести технологии на новый уровень, но и вписать их в общественный уклад, в выработанную веками систему человеческих ценностей.

Читайте наш журнал.
Регистрируйтесь на наши мероприятия.
Следите за новостями на сайтах.
Оформляйте подписку на www.secuteck.ru/subscription

Электронная версия журнала www.secuteck.ru/imag





СИСТЕМЫ БЕЗОПАСНОСТИ

SECURITY AND SAFETY

Журнал для руководителей и специалистов в области безопасности

www.secuteck.ru

№ 2(158) апрель – май 2021

В НОМЕРЕ

Генеральный директор ООО "Гротек": Андрей Мирошкин

Издатель: Владимир Вараксин

Руководитель проекта: Наталья Матлахова

Консультант проекта: Марина Садекова

Главный редактор: Марина Бойко

Редакторы: Анастасия Разбойникова, Анна Миронова

PR-менеджер: Екатерина Кузьмина

Менеджеры: Анастасия Волынкина, Наталья Зинина, Татьяна Чаусова

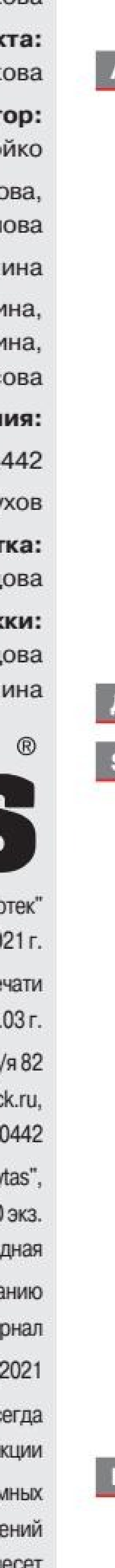
Департамент распространения: (495) 647-0442

Юрисконсульт: Кирилл Сухов

Дизайн, верстка: Ольга Пирадова

Дизайн первой обложки: Ольга Пирадова

Корректор: Галина Воронина



Учредитель и издатель ООО "Гротек"
Журнал "Системы безопасности" № 2 за 2021 г.
Издание зарегистрировано в Комитете РФ по печати
Свидетельство ПИ № 77-16428 от 22.09.03 г.
Для почты: 123007 Москва, а/я 82
www.secuteck.ru,
тел.: (495) 647-0442
Отпечатано: в ЗАО "Lietuvos rytas",
Вильнюс, Литва, тираж 25 000 экз.
Цена свободная

СИСТЕМЫ БЕЗОПАСНОСТИ
www.secuteck.ru
S&S
№ 2 (158) апрель – май 2021
SECURITY AND SAFETY
Журнал для руководителей и специалистов в области безопасности

В НОМЕРЕ



SECURITY AND SAFETY
Журнал для руководителей и специалистов в области безопасности

№ 2 (158) апрель – май 2021

В НОМЕРЕ



СИСТЕМЫ БЕЗОПАСНОСТИ
www.groteck.com
int@groteck.ru
№ 2(158) April – May 2021
S&S
SECURITY AND SAFETY
Industry Magazine for Security Professionals

FEATURES

ДЕЛОВАЯ ПРОГРАММА SECUTECK ONLINE 2021

Июнь 2021

1	Инновации в ритейле и e-commerce
3	Трансформация СКУД в биометрических проектах
8	Безопасность мест/объектов с массовым пребыванием людей
9	Интеллектуальные транспортные системы и элементы ситуационных центров
10	AgroTech: интеллектуальные технологии в сельском хозяйстве
15	Кибербезопасность цифрового предприятия
16	Современные решения для мультифакторной аутентификации
17	Антифрод и защита банковских систем
22	Цифровое ЖКХ и автоматизация зданий
23	Smart City. Будущее умных городов
24	Энергоэффективность: умное освещение в умном городе
29	Цифровая медицина: внедрение информационных технологий и кибербезопасность
30	Информационные технологии в металлургии и металлообработке



Годовая программа конференций
www.secuteck.ru/adapt

Высокоскоростная PTZ-камера AXIS Q6135-LE для съемки в темноте на большие расстояния

Axis Communications представляет высокоскоростную PTZ-камеру AXIS Q6135-LE с 32-кратным зумом, которая обеспечивает надежное видеонаблюдение в плохо освещенных местах на расстоянии до 250 м

Благодаря чипу нового поколения камера отличается улучшенным качеством изображения, расширенными функциями безопасности, широкими возможностями для аналитики и эффективным сжатием видеоизображения. Новая камера AXIS Q6135-LE отлично подходит для видеонаблюдения в парках, аллеях и других открытых пространствах в темное время суток. Функция Speed Dry обеспечивает эффективную очистку и позволяет получать четкие изображения в дождливую погоду.

Качество изображения

Камера оснащена адаптивной ИК-подсветкой дальнего действия с технологией OptimizedIR, которая настраивается в соответствии с масштабированием камеры, обеспечивая превосходное качество видео в темноте или при слабом освещении на расстоянии до 250 м и более в зависимости от сцены. Высокое качество изображения также достигается за счет технологии Lightfinder 2.0, благодаря которой можно получить насыщенные цвета и четкие изображения движущихся объектов в почти полной темноте. Еще одним достоинством камеры является технология Axis Zipstream с поддержкой форматов H.264 и H.265, которая значительно снижает требования к пропускной способности сети и емкости системы хранения без потери качества изображения.

Детальное отслеживание

Камера поддерживает динамическое наложение объектов для быстрой ориентации, а благодаря приложению Autotracking 2 с функцией запуска



слежения щелчком мыши можно прицельно отслеживать необходимые движущиеся объекты. Кроме того, с помощью приложения AXIS Object Analytics можно обнаруживать и классифицировать людей и транспортные средства. Эта первоклассная камера обладает также всем необходимым функционалом для отслеживания и выявления подозрительного поведения. В тех случаях, когда необходимо сохранить конфиденциальность, маскирование закрытых зон с помощью мозаичного узора позволяет пикселизировать целые участки сцены.

Гарантия киберзащиты

В AXIS Q6135-LE встроено ПО с цифровой подписью и функцией безопасной загрузки, что гарантирует защиту от каких-либо несанкционированных изменений. При необходимости функция безопасной загрузки обеспечит полное удаление вредоносного ПО после сброса параметров камеры к заводским установкам.

Камера оснащена также криптографическим модулем TPM (Trusted Platform Module), сертифицированным на соответствие стандарту FIPS 140-2, уровень 2. Данный модуль обеспечивает надежное хранение всех криптографических ключей и сертификатов и их неприкосновенность даже в случае взлома системы и нарушения защиты. ■

см. стр. 120 "Ньюсмейкеры"

30 лет на страже безопасности

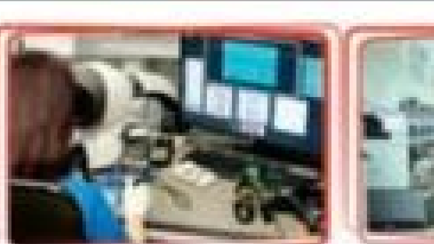
Компания "Болид" празднует свой 30-й день рождения. За это время наша компания стала одним из лидеров в разработке и производстве систем охранной и пожарной безопасности

Научно-внедренческое предприятие (НВП) "Болид" основано в 1991 г. Область деятельности – производство и поставка оборудования для систем безопасности, автоматизации и диспетчеризации.

За 30 лет компанией "Болид" запущено в крупносерийное производство более 450 наименований приборов и несколько десятков программных продуктов для создания систем пожарной и охранной сигнализации, пожарной автоматики, контроля доступа, видеонаблюдения, учета энергоресурсов, диспетчеризации и автоматизации инженерного оборудования.









Интегрированная система охраны "Орион", разработанная компанией "Болид", функционирует более чем на 1 млн объектов, обеспечивая безопасность населения России и ближнего зарубежья. Жилые дома, детские сады, школы, торговые центры, больницы, объекты культуры и искусства, аэропорты и промышленные предприятия, где установлено оборудование "Болид", надежно защищены от пожаров, краж, незаконных проникновений – оно обеспечивает комфортную и спокойную жизнь.

Продукция "Болида" получила всеобщее признание за свою надежность, доступную стоимость, широкую функциональность. Ежегодно внедряются новые инновационные разработки. Производство компании соответствует высоким мировым стандартам и оснащено передовыми технологическими линиями компаний FUJI, DEC, ERSA, NUTEC, ORBOTECH, ESPEC, SEICA, TERADYNE, PILLARHOUSE, включая автоматический поверхностный монтаж с трафаретной печатью и конвекционным оплавлением, пайку волной и автоматизированный многоступенчатый контроль качества на участках производственного процесса. Система менеджмента качества соответствует требованиям ГОСТ ИСО 9001–2015 (ISO 9001:2015).

Общий штат сотрудников превышает 800 человек, из них более 150 инженеров.

Ежегодный объем производства превышает 5 млн изделий, в которых применяются более 500 млн радиоэлектронных компонентов.

"Болид" – сплоченный, целеустремленный, единодушный коллектив сотрудников, мастеров своего дела, который гордится своими достижениями, богатыми корпоративными традициями и уверенностью в завтрашнем дне. ■

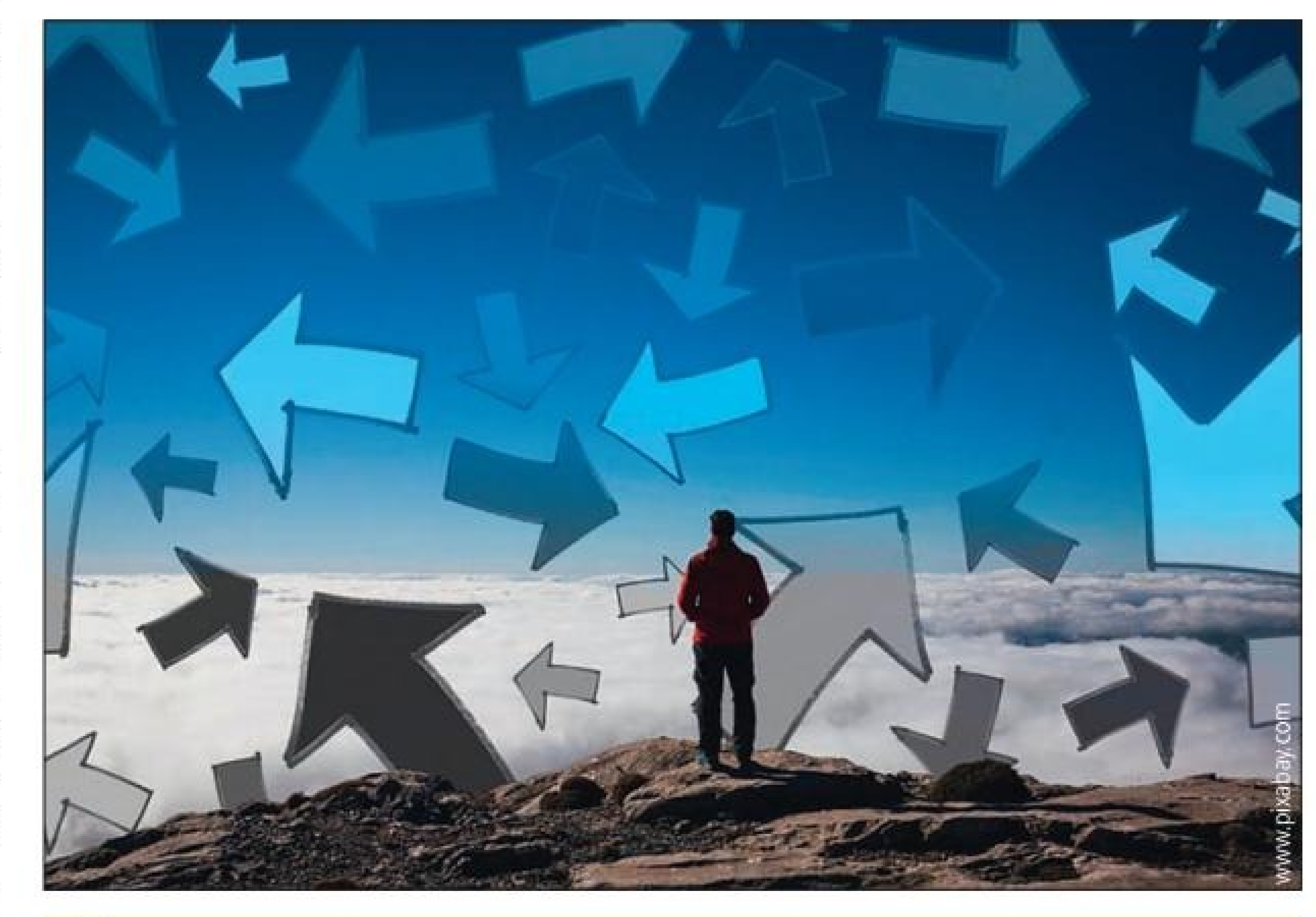
Источник: www.bolid.ru

Владимир Балановский
Член бюро комиссии РАН по техногенной безопасности, действительный член АПК и ВАНКБ, профессор Академии военных наук

Владимир Подъяконов
Научный сотрудник Научно-исследовательского отдела (военно-гуманитарных исследований) Военного университета МО РФ, член комиссии РАН по техногенной безопасности, к.и.н.

Специфические особенности оценки уязвимости общественной безопасности в условиях "управляемого хаоса"

Гибридные войны с применением технологий "управляемого хаоса" затрагивают все стороны жизни общества и, активизируя "протестный потенциал "пятой колонны", формируют условия для дестабилизации обстановки. Противодействие этому процессу начинается с оценки уязвимости гуманитарной сферы общественной безопасности. Центральным этапом такой работы является создание модели нарушителя. В его роли и в форме "мягкой силы" выступает "управляемый хаос", формирующий внутренних нарушителей, с помощью которых планируется разрушение нашего государства



В настоящее время США переводят противоборство в новые сферы. Мнение советника министра обороны РФ Андрея Ильницкого: "В классических войнах целью является уничтожение живой силы противника, целью новой войны является уничтожение самосознания. Этот тип войны – ментальный". Как при кибервойне, один вирус переходит в другой – из опознаваемого в виртуальный, но смертоносный, потому что внедряется не в разум, где его разумом можно разрушить, а именно в самоощущение, в удовлетворенность людей своей жизнью.

В классических войнах целью является уничтожение живой силы противника, целью новой войны является уничтожение самосознания. Этот тип войны – ментальный

Вектор противодействия смещается

Используя в качестве аналога апробированную модель борьбы с коронавирусом, необходимо выполнить профилактические "массовые прививки", что подтверждают слова заместителя председателя Госдумы Петра Толстого: "Мы все еще находимся в обороне, 30 лет мы отступали. Пора переходить в наступление. Основной фронт противостояния проходит на ментальном уровне, на ценностном..." Необходима суверенизация Интернета и подготовка кадров для информационного противодействия, необходимо обеспечить "выявление и лечение заболевших вирусной болезнью" – "нарушителей". В терминах противодействия актам незаконного вмешательства это люди, совершающие противоправное действие (бездействие), в том числе террористический акт, угрожающий безопасности жизненно важных интересов личности, общества, государства, повлекший за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавший угрозу наступления таких последствий.



Модели угроз и защиты от них

Вектор направлений разработки систем безопасности при этом смещается от противодействия терактам к противодействию внутренним нарушителям – части населения, живущей самоощущениями, людям с девиантным, отклоняющимся поведением. Эти люди являются противниками РФ в "ментальной войне", они основа протестного движения, формируемого "управляемым хаосом". Отклоняющееся поведение, враждебность и самоощущения у легко внушаемых людей "с отклю-

[1] *Макушкина О.А., Полубинская С.В. Предупреждение общественно опасных деяний, совершаемых лицами с психическими расстройствами: организация, статистические показатели, тенденции развития // Всероссийский криминологический журнал. 2019. Том 13. № 5.*

ченным разумом" (недостаточно образованных, без критического, но с "клиповым" мышлением) являются продуктом социальных процессов в России в 1991–2000 гг. Это вызвано сложившимся комплексом норм, морали, убеждений, ценностей и очарованности, которые действуют и до сих пор в качестве "окна" для фильтрования информации и определения ее значимости.

Формирование "псевдореальности"

При формировании в человеке, подверженном внешнему воздействию, "псевдореальности" – насильно созданного самоощущения, используется психосоматическая философия как основа "управляемого хаоса". Это позволяет осуществлять саморазрушение населения, то есть биологический суицид. Английский историк Тойнби говорил, что цивилизации погибают не от внешнего насилия, а от суицида, который развивается внутри цивилизации. Для целенаправленного разрушения РФ "псевдореальность" формируется с использованием биологических, социальных и психологических причин, влияющих на развитие и закрепление агрессии.

Как "взращиваются" внутренние нарушители

В качестве основы асоциальных групп задействуются люди с резко выраженным неадекватным поведением и активной агрессией. Такие аномалии характера неизбежно приводят к психопатии[1]. Яркими представителями таких "ядерных" психопатий являются диссоциальные психопаты, которых в прошлом называли "социопатами", "врагами общества". Эта категория, четко структурированная с помощью "управляемого хаоса", – основа "пятой колонны" – движения внутренних нарушителей для реализации актов незаконного вмешательства в РФ. Общественный строй изменился, но люди с психическими отклонениями остались, и ряды их из-за нестабильности общественно-политической, экономической, а теперь и эпидемиологической обстановки расширились, что стало находкой для "управляемого хаоса".

Анализ гуманитарной сферы РФ показывает, что уже возникли прямые угрозы самоощущению социума. Лидеров протестного движения спецслужбы США специально подготавливают с использованием психотропных средств, стимулирующих развитие астенических психических состояний и импульсивных моделей поведения. Это истеричные люди, имеющие подвижную психику, готовые при необходимости "завести" себя и исполнить роль "торпеды" для нанесения первого удара. Их сохранность в последующем необязательна, так как это расходный материал. А вот при формировании широкого фронта нарушителей используются плохо социализирующиеся люди с неярко выраженными отклонениями. При воздействии на них используют "психологические операции", направленные на индивидуальное и массовое сознание, чтобы посеять как можно больше неразберихи и беспорядка.

Арсенал психологического оружия

Для выявления аномалий поведения, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей в РФ, выработки и реализации методов контроля их сознания Агентством передовых оборонных исследовательских проектов Министерства обороны США DARPA еще в 2015 г. разработана программа "Выявление аномалий поведения" – Anomaly Detection at Multiple Scales (ADAMS). Информационно-психологическое воздействие на неадекватных людей, выявляемых ею, производится с помощью психологического оружия, позволяющего осуществлять влияние на общественное мнение, сознание, подсознание, психическое состояние населения с целью целенаправленного управления поведением. Совместно с информационно-психологическим используются также такие виды психологического оружия, как лингвистическое, психотронное, психофизическое, психотропное, сомато-психологическое. Отдельным видом является когнитивное оружие – внедрение теорий для ослабления государственного управления, вброс ложных сведений о тенденциях развития науки.

Вектор направлений разработки систем безопасности смещается от противодействия терактам к противодействию внутренним нарушителям. Отклоняющееся поведение, враждебность к обществу у легко внушаемых людей с "отключенным разумом" и "клиповым" мышлением являются продуктом социальных процессов в России в 1991–2000 гг.

Адекватные меры против "управляемого хаоса"

При оценке уязвимости гуманитарной сферы общественной безопасности РФ в качестве рекомендаций необходимо отметить, что противодействовать "управляемому хаосу" можно только с помощью адекватных средств. С этой целью формируется база данных лиц с девиантным поведением и создаются информационно-аналитические системы для противодействия манипулированию сознанием с использованием программы ADAMS. Выявление реализаторов актов незаконного вмешательства производится через модель нарушителя с применением информационных систем обеспечения оперативно-розыскных мероприятий (СОРМ), использующих сертифицированные технические решения согласно Федеральному закону № 374-ФЗ ("пакет Яровой"). Для повышения эффективности противодействия с помощью искусственного интеллекта проводится анализ, определение тенденций изменения, прогнозирование ситуации.

Предлагаемые для разработки информационно-аналитические системы должны получать в режиме реального времени информацию от информационно-аналитической системы, осуществляющей мониторинг и анализ СМИ и соцмедиа, а также от информационных систем лечебно-профилактических медицинских учреждений Минздрава и обмениваться ею с МВД и Росгвардией.

Основное внимание уделяется анализу судебно-психиатрической профилактики опасного поведения лиц, по своему психическому состоянию склонных к совершению общественно опасных действий либо создавших угрозу их наступления. Нужно определить места зарождения и пути миграции групп лиц с девиантным поведением. Результаты анализа позволят осуществлять деятельность по улучшению психологической и социальной обстановки в регионах.

Необходимо создать системы безопасности для распознавания фактов применения психологического оружия в местах массового скопления людей, разработать средства противодействия психотропным средствам в виде аэрозолей для скрытого воздействия в толпе, сомато-психологическому оружию для воздействия на сотрудников силовых служб, а также разработать средства безопасного противодействия общественно опасным деяниям:

- средства обездвижения (быстро затвердевающие составы, приклеивающие к технике, друг к другу, и суспензии, затрудняющие передвижения);
- "психологические заграждения" (генераторы шума, распылители составов с неприятным запахом).

Действовать безотлагательно

В условиях "ментальной войны" и "управляемого хаоса" необходима безотлагательная разработка и реализация вышеприведенного комплекса мероприятий, направленных на обеспечение защиты от угроз общественной безопасности. Совершенствование законодательства и нормативной базы позволит противодействовать радикальным элементам с отклоняющимся поведением в реализации ими внешнего заказа по дестабилизации морально-психологического состояния населения для развала России. ■

Необходимо создать системы безопасности для распознавания фактов применения психологического оружия в местах массового скопления людей, разработать средства противодействия психотропным средствам в виде аэрозолей для скрытого воздействия в толпе, сомато-психологическому оружию для воздействия на сотрудников силовых служб и др.

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Рынок тепловизионных систем: тенденции, влияние COVID-19 и прогноз на 2021–2026 годы

Обзор отчета исследовательской компании Mordor Intelligence

Рынок тепловизионных систем оценен в 5,19 млрд долларов в 2020 г., и ожидается, что достигнет 7,92 млрд долларов к 2026 г. при среднегодовом темпе роста 7,8%.

Инфракрасные и тепловизионные системы прошли через сдвиг парадигмы в последние годы из-за их все более широкого использования в военных и оборонных сферах. Многие страны вкладывают значительные средства в системы ИК и тепловизоров, чтобы справиться с глобальной политической нестабильностью и укрепить свою военную мощь, при этом глобальная напряженность постоянно растет, что стимулирует спрос на эти системы.



Тепловизоры все более широко применяют в военной и оборонной сферах

Драйверы рынка

Аналитики провели сегментацию рынка тепловизионных систем по сфере применения (термография, военные системы, видеонаблюдение, системы персонального зрения, пожаротушение, смартфоны), форм-фактору (портативные устройства формирования изображений, стационарные системы).

Исследования позволяют сделать следующие выводы:

1. Активно развиваются миниатюрные инфракрасные и тепловизионные датчики: благодаря достижениям в технологиях повышается их эффективность и упрощается использование. Портативные инфракрасные и тепловизионные системы привлекают внимание своей компактностью и находят применение в различных отраслях промышленности, таких как больницы, что позволяет, для примера, сократить время ремонта и расходы на отопление.

2. Такие факторы, как растущий спрос на видеонаблюдение в различных сферах деятельности, постепенное снижение стоимости тепловизионных камер и быстрое развитие высокоскоростных инфракрасных камер, приводят к увеличению спроса на ИК-камеры и позволяют демонстрировать рынку стабильный рост. Однако неточные измерения и ошибки с цветностью изображения, связанные с камерами, притормаживают этот процесс. Отрасли промышленности, в значительной степени полагающиеся на ИК-камеры, – это военная, оборонная и автомобильная промышленности.

3. Ожидается, что в ближайшие пять лет использование тепловизионных систем в автомобилестроении будет набирать обороты. Все более широкое использование тепловизионных камер в автомобильном секторе для снижения рисков при вождении, особенно в ночное время, является одной из основных причин роста рынка тепловизоров для автомобильной промышленности.

4. Региональные, национальные и международные аэропорты на сегодняшний день являются одними из основных целей для криминальных и террористических элементов. Персонал и ценное оборудование нуждаются в защите, в связи с чем наблюдается рост спроса на тепловизоры в аэропортах и в общественных местах.

5. Вспышка коронавируса COVID-19 нарушила цепочку поставок во всем мире, особенно в компаниях, производящих оборудование, электронику и полупроводники. Однако рыночный спрос на тепловизоры, определяющие температуру тела человека, вероятно, увеличится, и несколько игроков уже запускают новые продукты. Например, в мае 2020 г. Honeywell представила тепловизор с поддержкой искусственного интеллекта, который обнаруживает повышенную температуру тела человека у входов на фабрики, в аэропорты, распределительные центры и другие здания.

Ключевые тенденции

1. Ожидается, что рынок будет продолжать расти вместе с ростом инвестиций оборонного сектора в системы видеонаблюдения, ИК- и тепловизионные системы.

2. Повсеместно в военном секторе вкладывают средства в совершенствование технологий с целью предоставления военнослужащим более подробной и точной информации. Больше всего от этого выиграли коротковолновые ИК-камеры.

3. Во всем мире наблюдается тенденция роста преступности и насилия. Этот фактор привел к увеличению бюджета сил национальной безопасности на приобретение передовых систем защиты и устройств.

Северная Америка удержит самую большую долю рынка

Ожидается, что Северная Америка будет занимать значительную долю рынка ИК- и тепловизионных систем в течение прогнозируемого периода (2021–2026 гг.) из-за растущего внедрения этих продуктов в такие сферы, как мониторинг и обнаружение угроз, автомобильная промышленность, профилактическое обслуживание техники и др.

Ориентируясь на высокий спрос, вендоры разрабатывают новые продукты или решения. Например, компания FLIR Systems недавно выпустила комплект, включающий высокопроизводительную тепловизионную камеру для автопроизводителей и передовую систему помощи водителю.

Продолжается гонка технологий: большинство компаний стремятся разработать лучшую ИК-камеру с детализированным инфракрасным изображением, чтобы получить конкурентное преимущество. Например, Telops представила высокоскоростную инфракрасную камеру с максимальной пропускной способностью более 1 гигапикселя. Инфракрасная камера может получать изображение со скоростью 1900 кадр/с в полном разрешении, которое может быть увеличено до 90 тыс. кадр/с в специальном режиме (64x4 пксл).

Рынок сегодня

Рынок тепловизионных систем сегодня сконцентрирован в руках нескольких доминирующих игроков, среди них FLIR Systems, Raytheon Company, Opgal Optronic Industries, Fluke Corporation, Testo.

Постоянное внедрение инновационных решений требует от разработчиков лучшего понимания производственного процесса, чтобы предлагать подходящие решения и быстро оптимизировать производство. Компании также постоянно пытаются увеличить долю рынка за счет слияний и поглощений.

Некоторые из последних событий на рынке:

1. Декабрь 2019 г. Компания Raytheon строит два дополнительных комплекта радаров SPY-6 по контракту на 250 млн долларов с ВМС США. Компания заключила контракт на поставку в общей сложности девяти корабельных радаров для эсминцев DDG-51 Flight III.

2. Март 2020 г. Поставщик тепловизионных продуктов Seek Thermal представил Seek Scan™, простую и недорогую тепловизионную систему, предназначенную для автоматизации проверки температуры тела. Seek Scan специально разработан и откалиброван для обеспечения точных измерений температуры кожи при одновременном использовании протоколов социального дистанцирования.

3. Компания L-3 Communications, базирующаяся в Соединенных Штатах, запустила новейшие системы Warrior Systems (ALST). Компания также выпустила лазерный целеуказатель с дальномером и инфракрасный тепловизор, обеспечивающий точное целеуказание днем, ночью и в любых условиях боя. ■

По материалам www.mordorintelligence.com

"АСТРОН ПТР-2020": вижу все потоки

Представляет ОКБ "Астрон" www.astrohn.com

АСТРОН



Появление на рынке	I квартал 2021 г.
Ценовой сегмент	Средний

Решаемые задачи

Комплекс бесконтактного определения в потоке людей с повышенной температурой.

Конкурентные преимущества

Компьютер и ПО на основе нейронной сети распознают в потоке людей части тела для детектирования температуры, а именно лобную часть лица человека. Определяют температуру человека, игнорируя иные источники тепла, например кружку с горячим напитком, чтобы не допускать ложных сигналов тревоги. Интеллектуальный функционал включает в себя распознавание лиц людей, отслеживание пересечения виртуальных границ, направления движения и др.

Основные характеристики

- Разрешение тепловизионной матрицы/выходного тепловизионного изображения – 320x240 пкс.
- Спектральный диапазон – 7–14 мкм.
- Чувствительность NETD – 40 мК.
- Угол поля зрения телевизионного и тепловизионного канала – не менее 30 град.
- Измерение температуры в диапазоне +30...+45 °C.
- Функция калибровки по потоку людей (для относительного измерения температуры).
- Точность измерения относительной температуры без АЧТ – 0,3 °C.
- Видеосжатие – H.264, MJPEG.
- Поддержка ONVIF (опция).
- Действия по тревоге – "сухой контакт", фотоснимок, загрузка на FTP, запись на диск.
- Помощь в интеграции и сервисная поддержка в течение 24 месяцев.
- Потребляемая мощность – 12 Вт.
- Дополнительная камера видимого диапазона.

Возможности видеоаналитики

До 100 человек одновременно.

Интеграция

Открытый API, SDK.

Экономическая эффективность

Ключевые составляющие комплекса "АСТРОН ПТР-2020" (оптика, тепловизионный модуль и ПО) являются полностью российскими продуктами, что обеспечивает гарантию отсутствия утечек и конфиденциальность. ■

Проекты

Аэропорт Магадана, Государственная Дума, медучреждения г. Лыткарино

см. стр. 120 "Ньюсмейкеры"

Пирометр PERCo-AT01 для бесконтактного измерения температуры

Представляет PERCo www.perco.ru





Появление на рынке	Январь 2021 г.
Ценовой сегмент	Средний

Решаемые задачи

Пирометр PERCo-AT01 предназначен для бесконтактного измерения температуры открытых участков тела человека, например, запястья или ладони, на проходных предприятий, бизнес-центров и других объектов пребывания людей. Работает также в качестве верифицирующего устройства в составе СКУД.

Конкурентные преимущества

Основные отличительные особенности пирометра AT01 – высокая скорость и точность измерения, а также автоматизация контроля температуры и аппаратное взаимодействие со СКУД.

Основные характеристики

Точность измерения пирометра – ±0,2 °C в пределах диапазона измерения +36...+38 °C.
Скорость измерения – 1 с.
При выявлении сотрудника с повышенной температурой тела пирометр передаст в контроллер соответствующую информацию, и преграждающее устройство получит от контроллера команду на запрет прохода. Информация о событии прохода будет зафиксирована в системе. Система автоматически уведомит оператора о необходимости прохождения сотрудником медицинского освидетельствования. Если допуск к работе не может быть предоставлен, система сформирует сообщение об уважительной причине отсутствия на рабочем месте.

Возможности интеграции

Пирометр AT01 работает совместно с турникетом или замком. Для крепления пирометра к поверхности в комплект поставки входит металлическое основание. Взаимодействие со СКУД осуществляется посредством выхода "Открытый коллектор" или по интерфейсу Wiegand.

Экономическая эффективность

В отличие от ручных пирометров данная модель является автоматизированной, но значительно более бюджетной, чем тепловизор. Помимо этого, процесс измерения температуры не требует участия сотрудника, что снижает риск заражения. ■

Проекты

Самарская кабельная компания, Тверская швейная фабрика, "КДВ Павловский Посад" (Москва), офис PERCo (Санкт-Петербург), завод PERCo (Псков)

см. стр. 120 "Ньюсмейкеры"

Тепловизоры для быстрого определения температуры с нами надолго

Без всякого сомнения, в связи с пандемией коронавируса развитие технологий в сфере тепловидения пошло большими шагами. Рост потребности в противоэпидемических тепловизорах в 2019–2020 гг. был взрывным. Как следствие, увеличение производства таких тепловизоров вызвало всплеск развития технологий, которое коснулось как аппаратной, так и программой части



Дмитрий Шатунов
Заместитель генерального директора по производству ОКБ "АСТРОН"



Рост потребности в противоэпидемических тепловизорах вызвал всплеск развития технологий

Технические новшества

Например, в аппаратной части тепловизионной матрицы для противоэпидемических целей прекратили свой безудержный рост размеры. Выяснилось, что для целей определения температуры человека не нужны дорогие матрицы типа 1025x768 пкс или даже 640x480 пкс, вполне достаточно разрешения 320x240 пкс, но они должны быть гораздо дешевле, чем сейчас. Над этим работает большинство производителей микроболометров, создание которых, несмотря на все успехи, остается процессом дорогим и сложным. В идеале нужно, чтобы изготовление микроболометра от начала до конца велось с применением групповых технологий, на одной пластине, в едином цикле.

Кроме того, выросло многообразие формфакторов для тепловизоров. Сейчас можно встретить рамки металлоискателей со встроенными тепловизорами.

В программной части изменения более заметны. Задачи, решаемые большинством комплексов: бесконтактное измерение температуры человека, контроль ношения масок, соблюдения социальной дистанции, автоматизация управления проходом на охраняемые территории. Современные хорошие видеокомплексы измеряют температуру в непрерывном режиме, индивидуально или в потоке людей с надетыми медицинскими масками. Камера способна захватывать от нескольких человек до десятков "целей" в кадре одновременно, почти мгновенно с высокой точностью определяя температурные показатели. Система отображает результаты измерений на экране видеомонитора оператора в виде числовых значений и цветных рамок вокруг лиц людей. Она интегрируется со СКУД на данном предприятии. Камеры-тепловизоры с видеоаналитикой определяют температуру человека, игнорируя иные источники тепла, например кружку с горячим напитком, чтобы не допускать ложных сигналов тревоги. Интеллектуальный функционал может включать в себя распознавание лиц людей, отслеживание пересечения виртуальных "границ", направления движения и др.

Мы на пороге революции

В основе новых решений – передовые тепловизионные технологии и искусственный интеллект на базе тепловизоров. К тепловизионным технологиям можно отнести, например, функцию совмещения двух спектров. Это используется для более точного определения событий и объектов. Она придумана не в 2020 г., но стала широко использоваться именно сейчас. Увеличенное разрешение оптического модуля обеспечивает детализацию кадра, а тепловизионный модуль отвечает за мониторинг ночью. Оптическое и тепловизионное изображение можно просматривать как по отдельности, так и в формате наложения кадров (так называемая технология Fusion). Тепловизионный спектр эффективен для охранного мониторинга в темное время суток или в плохих погодных условиях (туман, осадки), а оптический канал дает возможность оператору комфортно работать днем в хорошую погоду. Эта группа устройств "два в одном" совмещает в едином корпусе тепловизионный модуль и камеру видимого диапазона. Такие видеокомплексы от Smartec, Wisenet/Hanwha Techwin, ОКБ "Астрон", НПП "Александр" и другие передают не только тепловое изображение, но и обычную картинку высокого разрешения для верификации событий и внесения лиц в базу данных.

Искусственный интеллект (ИИ) продвигается во все значимые сферы жизни. Технологии становятся доступнее, их применение – гибче. Например, можно провести распознавание лиц, атрибутов людей, машин, типов объектов, анализ поведения. Все это доступно как для телевизионного канала, так и для тепловизионного. Мы действительно на пороге революции, по итогам которой ИИ и большие данные станут основными драйверами роста.

Главные заказчики

По нашему опыту, основными потребителями тепловизионной техники в 2020 г. были государственные учреждения. На втором месте идут гостиничные комплексы, далее – аэропорты и вокзалы. В целом в силу специфики 2020 г. высокую активность проявляли предприятия из основных сегментов – производства, торговли и социально значимые организации.

Будущее "коронавирусных" тепловизоров

Спрос резко вырос, и небольшой сегмент рынка тепловизоров для точного измерения температуры, который совсем недавно в мире занимал около 20%, а в России – около 1% от всего количества тепловизоров, превратился в большой и важный. Видимо, он измеряется несколькими десятками процентов. Спрогнозировать объемы рынка тепловизионных регистраторов температуры, применяемых в сфере эпидемиологической безопасности, довольно сложно. Слишком много факторов, которые будут влиять на динамику рынка. Например, будет ли закреплено в государственных стандартах и программах обязательное использование стационарных тепловизионных регистраторов?

Что произойдет, когда пандемия так или иначе будет взята под контроль? Означает ли это, что по окончании пандемии актуальность проблемы создания правильного медицинского тепловизора для контроля потоков людей потеряет свою актуальность?

Думается, что развитие медицины пойдет по пути создания диагностирующих комплексов, в которых термография будет одним из элементов диагностики. Так, в 2020 г. специалисты Фраунгоферовского института машиностроения и автоматизации разработали установку, способную с расстояния в 1 м выявить основные симптомы COVID-19 – повышенную температуру, учащенное сердцебиение и сниженный уровень кислорода в крови. Температура тела измеряется с помощью тепловизора, а вот для определения двух других симптомов немецкие специалисты применили микроволновый радар. Он улавливает движения и вибрации грудной клетки, вызываемые дыханием и сердцебиением. Таким же образом определятся и частота сердцебиения.

Все это означает, что тепловизор для корректного и быстрого определения температуры человека в потоке людей – новая реальность очень надолго.

ЭКСПЕРТИЗА, МНЕНИЯ





Пандемия создала хайп в тепловидении

Что точно сделала пандемия с тепловидением в 2020 г., так это создала хайп. Простыми словами, ничего нового в плане прорыва тепловизионных технологий не произошло, однако появилась возможность хорошо заработать в период хайпа (февраль – сентябрь 2020 г.) и продвинуть в массы само слово "тепловизор". А в дальнейшем из технологий реально будут работать и использоваться СКУД-панели с датчиком температуры и доступом по распознаванию лиц

Дмитрий Карнеев
Генеральный директор
компании KARNEEV SYSTEMS

Появление неимоверного количества приборов формата "тепловизор + камера распознавания лиц" – не более чем хайп волны ковида. Работают такие приборы с определенной долей вероятности правильного обнаружения больных, при этом нужно соблюсти большое количество технических правил установки и организационных условий направления потока людей на проходных. В общем, решение с тепловизорами более-менее рабочее, но при огромном количестве "но". Безусловно, ковид подстегнул развитие технологий СКУД в плане того, что возник спрос на новые функции, а это подтянуло конкуренцию и, в свою очередь, развитие технологий СКУД для победы в конкурентной борьбе. В этом можно увидеть заслугу ковидного тепловизионного хайпа.

Появление неимоверного количества приборов формата "тепловизор + камера распознавания лиц" – не более чем хайп волны ковида. Работают такие приборы с определенной долей вероятности правильного обнаружения больных, при этом нужно соблюсти большое количество технических правил установки и организационных условий направления потока людей на проходных

Через 10 лет посмотрим

Тепловизоры – одна из основных специализаций нашей компании, поэтому все тренды и новинки в этой области нам хорошо известны. И тут я не смогу конкретно выделить 2020 г. как время прорыва в тепловизионных технологиях. Развитие тепловизоров все еще идет по принципу уменьшения размера пикселя детектора, увеличения разрешающей способности и снижения финальной стоимости конечного изделия. Этот процесс будет продолжаться, с моей точки зрения, еще около 10 лет.

Развитие тепловизоров все еще идет по принципу уменьшения размера пикселя детектора, увеличения разрешающей способности и снижения финальной стоимости конечного изделия. Этот процесс будет продолжаться, с моей точки зрения, еще около 10 лет

Дополнительный канал информации

Сферы применения тепловизоров уже хорошо знакомы и изучены. Наиболее перспективной выглядит область, связанная не с видеонаблюдением, а с температурными аспектами использования тепловизоров для привлечения дополнительного канала принятия решений в общую базу знаний для интеллектуальных функций улучшения бизнеса предприятий. В этом вижу перспективу развития именно тепловизионной технологии как средства решения проблем клиентов. Традиционные рынки наблюдения с тепловизорами развиваются и матереют вместе с обычным видеонаблюдением, и здесь я бы не стал как-то отдельно выделять тепловизоры. Это всего лишь дополнительный канал видеоинформации, который не зависит от освещенности объекта.

www.karneev.com

Традиционный тепловизонный рынок не претерпел каких-либо существенных изменений. На фото – тепловизионный мониторинг обнаружения шлака

Тепловизонные рынки все те же

Хайповый тепловизионный 2020 год – это год приборов для рынка пандемии, о нем я говорил выше. Традиционные тепловизонные рынки не претерпели каких-либо существенных изменений, все движется так, как и должно, а 2021 год это прекрасно доказывает своими продажами и проектами. Постепенно мы перестанем рассматривать тепловизоры отдельно от каких-либо других технологий безопасности. Почему бы не спросить: а кто был основными потребителями периметральной сигнализации в 2020 г.? Те же, кто и в 2019 г., и в 2021 г.! Это сложившиеся, заматеревшие рынки. Тепловизоры все еще немного дороги, поэтому мы их рассматриваем отдельно, но постепенно перестанем это делать. Просто нужно еще время.

"Коронавирусные" тепловизоры жестко конкурируют с панелями доступа и... проигрывают. Ниша таких тепловизоров останется там, где априори нельзя поставить панель доступа

Панели доступа выигрывают

"Коронавирусные" тепловизоры жестко конкурируют с панелями доступа и... проигрывают. Ниша таких тепловизоров останется там, где априори нельзя поставить панель доступа. По сути, панели дешевле, точнее, дают множество дополнительных функций и стоят там, где и должны быть: на месте, где необходимы проверка и допуск или отказ в допуске, – на КПП. Безусловно, "коронавирусные" тепловизоры останутся, но спрос на них будет невелик, ибо: а) есть решение лучше – панель доступа, б) очень много "но" и того, что надо учесть и сделать, чтобы такой тепловизор более-менее нормально выполнял свою задачу. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Кардинальные изменения на рынке тепловизоров маловероятны



Николай Чура
Технический консультант
компании "Фирма "Видеоскан"

Серьезное стимулирование технологий в сфере тепловидения в пандемию весьма маловероятно. На это есть сразу несколько причин.

На протяжении пандемии, которой нет и 1,5 лет, даже при существующей стремительности технического развития относительно мало что может быть кардинально усовершенствовано.

Массовые и специализированные решения по экспресс-контролю температуры

Сам по себе режим пандемии с изменением форматов работы, сокращением связей, да и с почти тотальным уменьшением спроса на оборудование также не усилил интенсивность разработок и производства. Можно отметить лишь более широкое применение оборудования для скоростного дистанционного измерения температуры человека.

Пандемия, даже с учетом сильного сокращения пассажиропотоков, поставила серьезную задачу экспресс-анализа температуры тела человека и определения ее носителя в этих потоках.

Те немногие сообщения о потенциальном применении тепловизоров для экспресс-контроля температуры проходящих людей поначалу носили скорее рекламный и популистский характер. Вместе с тем такие системы стали появляться в международных аэропортах. Здесь, безусловно, надо учитывать страстное желание разработчиков и поставщиков тепловизоров освоить огромный рынок широких государственных поставок, используя массовую панику.

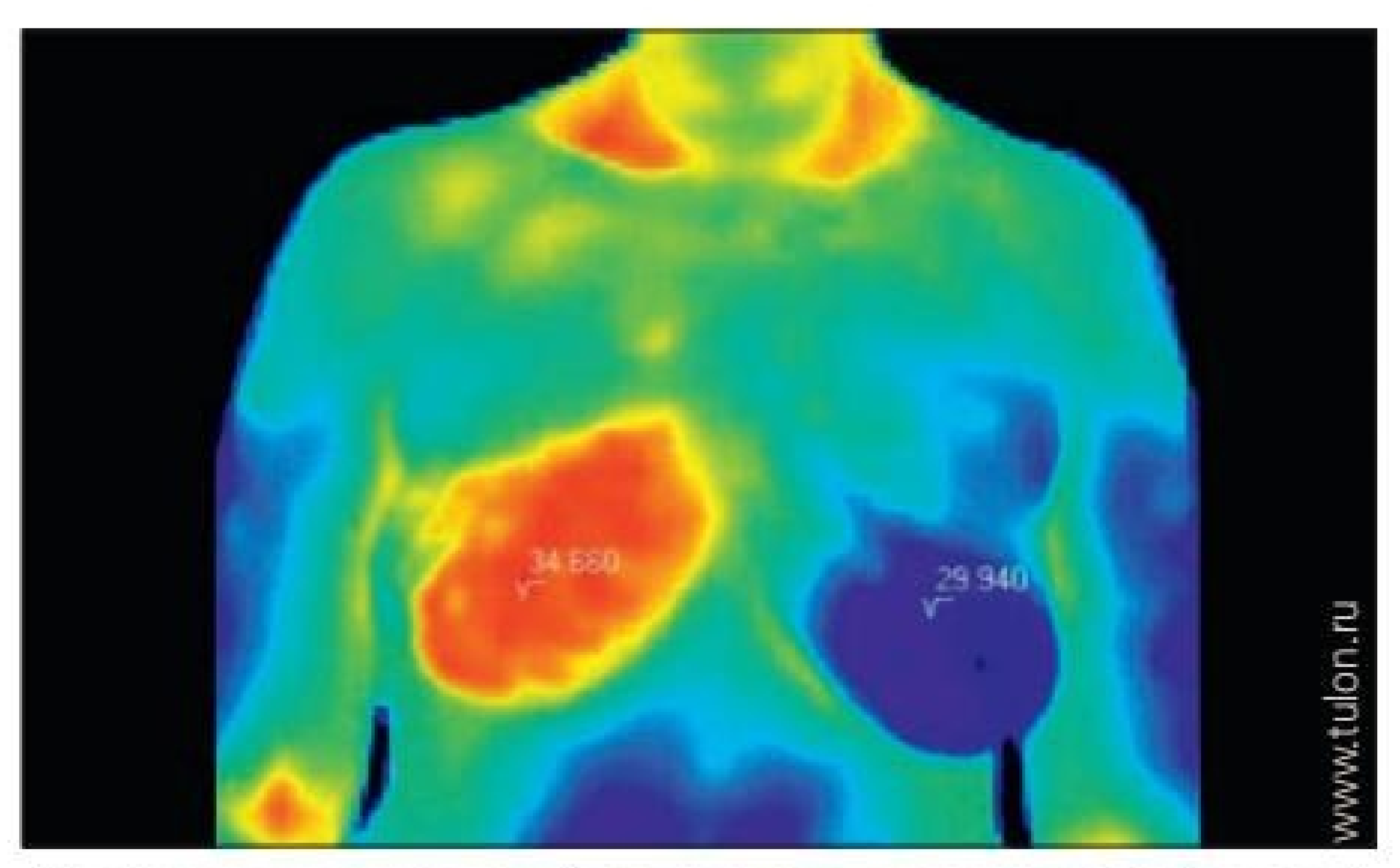
Относительно стимуляции развития самих тепловизионных технологий: в первую очередь она коснулась специализированной цифровой обработки изображений и адаптации уже существующих двухволновых систем (видимый и инфракрасный диапазон) для решения описанной задачи.

Подобный "суперкомплекс" российского поставщика имеет тепловую чувствительность 0,04 °С (NETD) со временем срабатывания 0,5 с, дальностью действия до 12 м и погрешностью ±0,5 °С. К сожалению, не указано, что это за погрешность и можно ли ее считать температурным разрешением или ценой деления термометра. Видимый телевизионный канал обеспечивает распознавание и регистрацию лиц в поле зрения устройства. В системе использованы технологии искусственного интеллекта как в распознавании лиц, так и в нормировании температурных измерений с текущей оценкой среднего значения температуры объектов. Цена его также не указана, но подобные комплексы имеют стоимость порядка 5–7 млн рублей. Сообщается, что за время пандемии по СНГ разошлось около 300 таких устройств.

Новые технологические направления

Не привязываясь конкретно к 2020 г., можно выделить два относительно новых направления термографии.

Первое – это попытки диагностики различных заболеваний с помощью обнаружения воспалительных процессов в теле пациента. Тепловизоры с соответствующей цифровой обработкой уже участвуют в клинических испытаниях. Однако, учитывая весьма посредственную прозрачность тканей человека для ИК-излучения, возможности этой методики, на мой взгляд, весьма ограниченные. Причем это справедливо даже для длинноволновой части тепловизионного диапазона (7–13 мкм), в котором и работает данное устройство.



Одно из новых направлений термометрии – диагностика заболеваний с помощью обнаружения воспалительных процессов в теле пациента

Второй технологией можно считать обнаружение утечек из трубопроводов и оборудования природного газа, нефти и нефтепродуктов. Варианты использования подобных методик обсуждались и моделировались еще в 1990-х гг. Но доступ к зарубежной высокочувствительной тепловизионной технике в те времена был крайне ограничен даже для структур "Газпрома", в которых я тогда работал. Российские же, а точнее советские приборы тогда были еще в экспериментальном, зачаточном состоянии и не могли реально конкурировать с зарубежными. Как, впрочем, и сейчас.

Сферы использования без изменений

Основными направлениями использования тепловизоров в 2020 г., как и в предыдущие годы, остаются:

- безопасность (обнаружение нарушителей);
- дистанционное обнаружение очагов возгорания;
- технологический контроль нагретых неисправных элементов;
- обнаружение утечек высокотемпературных сред;
- научная и исследовательская деятельность.

"Уникальные" устройства или традиционные термометры?

Естественно, "коронавирусные" тепловизоры как системы контроля температуры человека находятся в сегменте медицинского оборудования. Можно надеяться, что ручные дистанционные медицинские термометры и в дальнейшем вполне смогут находить применение. Бесконтактность (до 10 см) и быстрота измерения (0,5 с) с погрешностью около 0,2 °С, а также наличие сигнализации превышения заданного референтного порога (обычно около 37,3 °С) выгодно отличают их от традиционных ртутных или спиртовых термометров. В силу личных обстоятельств последний год я был вынужден регулярно посещать различные медицинские учреждения. Там у меня по нескольку раз в день на всех этапах контролировали температуру этими термометрами. Встречал я и некие консоли, определяющие наличие маски у посетителя и его температуру. Эти устройства всегда были китайского производства и чаще всего выдавали совершенно нереальный результат, а консоли были не в состоянии обнаружить и медицинскую маску на лице. Занимательно, что последние месяцы персонал в основном перешел на традиционные термометры.

Возможно, это объясняется слишком низкой ценой этих "уникальных" устройств – около 1500 рублей. И может быть, подобное оборудование от нашего основного и старейшего поставщика тепловизионной техники, но за 40 тыс. рублей, работало бы более адекватно. Но цена... Для справки: типовой термометр в аптеке стоит около 100 рублей.

Серьезные двухволновые системы, установленные сейчас в некоторых аэропортах, одна из которых рассматривалась в начале, после окончания пандемии навряд ли будут пользоваться большим спросом (если только пандемии не станут обыденным явлением). Вместе с тем подобные решения могут найти другое применение в различных отраслях после замены программного обеспечения.

ЭКСПЕРТИЗА, МНЕНИЯ




ALL-OVER-IP
Мощный гибридный формат
24-26 ноября офлайн
три недели праздника технологий онлайн
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ
СВЕРШИЛАСЬ
2021
www.all-over-ip.ru



Оксана Козлова
Директор по охране труда, промышленной безопасности и экологии АО "НИПИГАЗ" (г. Москва)



Александр Агошков
Профессор, вице-президент МАНЭБ (Международной академии наук экологии и безопасности жизнедеятельности), заведующий кафедрой "Безопасность жизнедеятельности в техносфере" Дальневосточного федерального университета, д.т.н.



Павел Курочкин
Менеджер по охране труда, промышленной безопасности и экологии АО "НИПИГАЗ" (г. Москва)

Как сдержать распространение инфекционных заболеваний на производственных и строительных предприятиях

В условиях оперативного принятия мер по недопущению распространения новой коронавирусной инфекции отечественные и зарубежные компании, работающие в России, столкнулись с необходимостью ускорения процессов выработки и реализации принятых решений, трансформации традиционных форм и практик ведения бизнеса в целях его сохранения и обеспечения надежного функционирования, выработки комплекса мероприятий по защите собственных сотрудников и работников подрядных организаций. Вызовы, обусловленные реагированием на COVID-19, позволили усовершенствовать организационно-методические инструменты управления рисками охраны труда в целях обеспечения бесперебойной работы производственных предприятий и строительных организаций, выявить возможности улучшения систем реагирования на чрезвычайные ситуации природного и техногенного характера

В данной статье систематизированы решения, применяемые крупными иностранными и отечественными компаниями для обеспечения надежности производственно-коммерческой деятельности в условиях разработки и реализации мероприятий по нераспространению острых респираторных вирусных инфекций, включая новую коронавирусную инфекцию, предложена методика реагирования на сезонную заболеваемость, эпидемию или пандемию на основе реализации комплекса организационно-методических мероприятий.

Влияние инфекционных заболеваний на деятельность производственных предприятий и строительных организаций

Анализ опыта реализации крупных инвестиционных строительных проектов в России (Ямал СПГ, проекты в Сибири и на Дальнем Востоке по освоению Салымского и Ванкорского месторождений, проекты на о. Сахалин) и за рубежом (Казахстан, Нигерия, Папуа – Новая Гвинея, Венесуэла), а также литературных источников[1, 2, 3] позволяют сделать следующие общие выводы:

- инфекционные заболевания различной природы (респираторные, кишечные, иные) негативно влияют на показатели производственных предприятий и строительных организаций вследствие потерь рабочего времени, привлечения дополнительных ресурсов для обеспечения производственной деятельности;
- во всех известных случаях заражение работников на предприятии явилось следствием контакта с работником, заразившимся в быту, вне работы (инфекция была принесена извне);
- инфекционные заболевания различной природы (например, грипп или кишечные заболевания) могут распространяться с высокой скоростью, поражая сотрудников, которые вынужденно находятся в непосредственной близости друг от друга;
- в условиях вахтового режима работы при размещении работников строительных организаций во временных вахтовых поселках риск негативного влияния на реализацию строительного проекта достигает неприемлемых значений (высокая вероятность одновременной потери трудоспособности большим количеством работников строительных организаций и ограниченности инфраструктурных, материальных, человеческих и иных ресурсов для минимизации негативного воздействия).

Полученный опыт негативного влияния новой коронавирусной инфекции на все сферы экономической жизни во многих странах мира подчеркивает важность и актуальность проработки вопросов организации реагирования на такие ситуации в целях минимизации последствий (репутационных, финансовых и др.).

Методика реагирования на сезонную заболеваемость, эпидемию или пандемию

Анализ подходов и методов обеспечения надежности производственной деятельности, используемый зарубежными и отечественными

Таблица 1. Рекомендации по информированию ответственных сотрудников о возникновении инфекционного заболевания

Количество зарегистрированных случаев	Заболевания
Зарегистрировано два (или более) случаев	Диарея и/или рвота (по любой причине). Подтвержденные случаи норовирусной инфекции или сальмонеллеза. Сезонный грипп
Зарегистрирован один (первый) случай заболевания	Туберкулез. Менингит. Холера. Легионелла. Ветряная оспа. Коронавирусная инфекция

[1] Robert H. Friis. Occupational Health and Safety for The 21st Century. Jones and Barlett Learning LLC, 2020. P. 429.
[2] David L. Goetsch. Occupational Safety and Health for Technologists, Engineers and Managers. Jones and Barlett Learning LLC, 2020. P. 239.
[3] Ron C. McKinnon. The Design, Implementation and Audit of Occupational Health and Safety Management Systems (Workplace Safety, Risk Management and Industrial Hygiene). Taylor & Francis Group, 2020. P. 232.

Таблица 2. Общая структура процесса (универсальный алгоритм действий) реагирования на возникновение и распространение инфекционного заболевания

Этап реагирования	До возникновения сезонного заболевания, эпидемии или пандемии	Во время распространения сезонного заболевания, эпидемии или пандемии	После сезонного заболевания, эпидемии или пандемии
Направленность мероприятий	1. Оценка потенциальных опасностей, обусловленных возникновением инфекционного заболевания. Разработка плана реагирования. 2. Мероприятия, направленные на повышение компетентности персонала (информирование о поведении, предотвращающем распространение заболевания, мерах и способах защиты и т.д.). 3. На основе данных оценки рисков: заключение договоров с медицинскими организациями, создание материально-технической базы для обеспечения реагирования на этапе распространения заболевания, подготовка необходимой инфраструктуры.	Реализация мероприятий плана реагирования на распространение инфекционного заболевания. 1. Изменение режима работы (если необходимо): перевод сотрудников офиса на удаленный режим работы, перевод производственных подразделений или объектов строительства в вахтовый режим работы. 2. Реализация мероприятий, сдерживающих распространение инфекции: медицинский осмотр и тестирование персонала (в зависимости от режима работы предприятия), в зависимости от особенностей производственной деятельности организация обсерваторов (до и после вахты), изоляторов (для персонала с симптомами заболевания), дезинфекция помещений, поверхностей, предметов общего пользования и т.д.	1. Расследование причин и развития инфекционного заболевания на предприятии или в организации. 2. Извлечение уроков из опыта, полученного в практике реагирования на распространение инфекционного заболевания. 3. На основании извлеченных уроков корректировка деятельности для минимизации негативного воздействия при возникновении подобных ситуаций в будущем.

Таблица 3. Основные мероприятия реагирования на возникновение инфекционного заболевания (универсальный алгоритм действий)

Этап реагирования	Мероприятия
До возникновения сезонного заболевания, эпидемии или пандемии – при получении информации о росте заболеваемости в регионе производства работ или информации об эпидемическом/пандемическом характере заболевания	Информирование сотрудников и работников строительных организаций, привлеченных к выполнению работ (например, в ситуации с коронавирусом – разработка памяток, фильмов, тренингов, инструктажей и др. по средствам защиты: использованию дезинфектантов, правильному использованию масок и перчаток, мытью рук и т.д.). Идентификация и оценка возможных рисков, разработка и подготовка реализации мероприятий. Выделение помещений для изоляции зараженного персонала (для производственных предприятий, вахтовых поселков и строительных организаций, переведенных в режим "короткой вахты"). Проработка вопросов ресурсного обеспечения наихудшего сценария (подготовка инфраструктуры, реализация предварительных мероприятий по обеспечению необходимыми средствами, например масками, перчатками, дезинфектантами, ноутбуками и т.д.)
Во время распространения сезонного заболевания, эпидемии или пандемии – сразу после регистрации максимально двух случаев заражения работников	Оповещение руководства организации и заказчиков работ в соответствии с требованиями табл. 4 (при регистрации не более двух случаев инфекционного заболевания). Определение лиц, контактировавших с заболевшими, обеспечение их изоляции. Медицинский осмотр и тестирование всех сотрудников подразделения предприятия или организации.Реализация мероприятий по обеспечению санитарно-гигиенических требований работниками (повышенное внимание мытью и дезинфекции рук, использованию средств индивидуальной защиты – масок и перчаток). Разработка и реализация мероприятий, сдерживающих распространение инфекции: ● уборка и дезинфекция помещений ● обеспечение питанием ● транспортировка работников, социальное дистанцирование, изолирование работников с подозрением на инфекционное заболевание, ограничение/исключение выполнения работ заболевшими работниками ● внутреннее расследование причин возникновения заболевания (максимально возможная детализация причин для извлечения уроков и предотвращения подобных ситуаций в будущем)
После сезонного заболевания, эпидемии или пандемии	Завершение внутреннего расследования причин возникновения заболевания. Извлечение уроков и корректировка деятельности

компаниями[1, 2, 3], позволил сформировать методику реагирования на угрозу возникновения и распространения инфекционного заболевания (респираторного, кишечного, иной природы) на основе реализации комплекса организационно-методических мероприятий (табл. 1, 2, 3).

Человеческий фактор и его влияние на эффективность мероприятий

Пример коронавирусной инфекции показал, что в отсутствие вакцины производственные предприятия и строительные организации смогли в кратчайшие сроки выработать и реализовать комплексы организационных, а в некоторых случаях организационно-технических, мероприятий по недопущению распространения COVID-19 и иных ОРВИ, эффективность реализации которых напрямую определяется фактическим состоянием и влиянием, которое оказывает человеческий фактор на производственно-технологический процесс (табл. 4).

Характеристики человеческого фактора и метод их количественной оценки описаны в экспертных статьях[4].

Рекомендации по организации внутреннего расследования причин возникновения заболевания

На этапе развития сезонного заболевания, эпидемии или пандемии необходимо сформировать комиссию по расследованию причин возникновения заболевания на предприятии. Это нужно для извлечения уроков и обеспечения надежной и бесперебойной работы в будущем. В комиссию целесообразно включать руководителя производственного подразделения, руководителей направлений, групп и отделов, специалиста по охране здоровья или сотрудника медицинской организации, оказывающей по договору соответствующие услуги.

Комиссии по расследованию сезонной заболеваемости необходимо обоснованно ответить на определенные вопросы (табл. 5).

Специалист по охране здоровья консолидирует полученную информацию, формирует проект отчета, рекомендации по организации работы предприятия или объекта строительства в

Таблица 4. Схема методики выполнения требований по нераспространению инфекционных заболеваний на основе управления влиянием человеческого фактора на производственно-технологический процесс

Этап методики/Результат	Мероприятия	
Этап 1. Оценка состояния производственно-технологического процесса. Результат: оценены фактические (санитарно-гигиенические риски) и их влияние на производственно-технологический процесс	Идентификация целевых параметров производственно-технологического процесса: ● формирование требований к охране труда и безопасности производственно-технологического процесса ● определение параметров приемлемости уровней общей заболеваемости	Определение и оценка фактических параметров производственно-технологического процесса: ● сбор данных для оценки производственно-технологического процесса ● оценка действующих факторов и существующих организационно-технологических условий выполнения работ
Этап 2. Оценка состояния человеческого фактора. Результат: оценено соответствие фактических характеристик параметров человеческого фактора целевым значениям	Определение целевых параметров характеристик человеческого фактора, обеспечивающих приемлемый уровень общей заболеваемости: ● уровень общей компетентности сотрудников и работников подрядных организаций ● уровень мотивированности сотрудников и работников подрядных организаций ● состояние полномочий и ответственности, согласно действующим инструкциям (справочник должностей, должностные инструкции и т.д.)	Выявление фактических характеристик человеческого фактора: ● оценка компетентности сотрудников и работников подрядных организаций ● оценка мотивации сотрудников и работников подрядных организаций ● оценка соответствия полномочий и ответственности согласно действующим нормативным и распорядительным документам (справочник должностей, должностные инструкции и т.д.)
Этап 3. Приведение фактических параметров характеристик человеческого фактора к целевым значениям для обеспечения выполнения требований	Выявление фактических характеристик человеческого фактора, оказывающих влияние на повышение риска высокой динамики общей заболеваемости (в том числе новой коронавирусной инфекцией и иными ОРВИ), для обеспечения надежного и бесперебойного функционирования производственно-технологического процесса (организации в целом). Определение адекватных способов изменения выделенных характеристик. Изменение выделенных характеристик (устранение несоответствий). Подтверждение достижения параметров характеристик человеческого фактора целевым значениям. Осуществление производственно-технологического процесса с приемлемым риском	

период развития заболеваемости. По завершении периода заболеваемости в отчет включается дополнительная информация по извлеченным урокам.

Цели проведения расследования заболеваемости:

- определить, каким образом инфекционное заболевание было занесено на территорию производственного предприятия или объекта строительства и какие мероприятия необходимо предусмотреть для исключения повторения таких случаев в будущем;
- определить рекомендации по изменению бизнес-процессов, текущей производственно-коммерческой деятельности для минимизации возможного негативного воздействия на показатели предприятия;
- распространить информацию о полученном опыте и выработанных рекомендациях (в случаях холдинговой организации бизнеса);
- скорректировать стратегии реагирования на угрозы общей сезонной заболеваемости, формирования практик управления рисками охраны здоровья и охраны труда.

В подавляющем большинстве случаев успешность мероприятий по профилактике распространения инфекционного заболевания зависит от эффективных действий, предпринятых в течение первых 48 часов с момента получения информации о максимально двух случаях заболевания на предприятии или на строительном объекте – именно в этот период времени необходимо собрать образцы для исследования в лаборатории.

Как отмечено ранее, к работам необходимо привлекать лабораторию, с которой установлены контрактные взаимоотношения на этапе до возникновения сезонного заболевания, эпидемии или пандемии.

Таблица 5. Основные вопросы, рассматриваемые комиссией по расследованию причин сезонного заболевания, эпидемии или пандемии

Вопрос	Ответственность за предоставление информации (кто формирует ответ на вопрос)
Случаи возникновения какого заболевания зарегистрированы и какими патогенами это заболевание вызывается?	Обычно специалист по охране здоровья или сотрудник медицинской организации. Информацию необходимо подтвердить данными лабораторных исследований
Наблюдается ли рост количества зарегистрированных случаев инфекционного заболевания в регионе производства работ или регионах, откуда прибывает вахтовый персонал?	Комиссия по расследованию
Насколько тяжелые последствия инфекционного заболевания (высокая контактность, тяжелые формы осложнений) и какие риск-факторы для обеспечения надежного функционирования производственного предприятия или строительной организации существуют?	Специалист по охране здоровья и/или специалист медицинской организации
Какие пути и факторы передачи инфекционного заболевания существуют?	Специалист по охране здоровья на основе информации от региональных органов Роспотребнадзора (в его отсутствие – сотрудник медицинской организации)

Обеспечить сбор биологического материала для проведения исследований необходимо так быстро, как это только возможно в существующих условиях. В ситуации, когда медицинское учреждение имеет в наличии тест-системы, включая экспресс-тесты, необходимо организовать тестирование персонала производственного предприятия или объекта строительства (в том числе работников всех подрядных и субподрядных организаций низшего звена). Ответственность за организацию тестирования несет руководитель предприятия и специалист по охране здоровья.

Простые меры – важные результаты

Основу предложенной методики составляют структурированные по этапам реализации простые организационные и методические мероприятия, позволяющие обеспечить эффективность профилактики распространения инфекционных заболеваний среди сотрудников. Предлагаемые меры просты в применении и при внедрении в деятельность предприятия не требуют дополнительного ресурсного обеспечения. ■

Ваше мнение и вопросы по статье направляйте на



[4] *Курочкин П.А. Методы учета влияния человеческого фактора в управлении производственными рисками // Газовая промышленность. 2019. № 10. С. 126–133.*

О слияниях и поглощениях на рынке систем безопасности

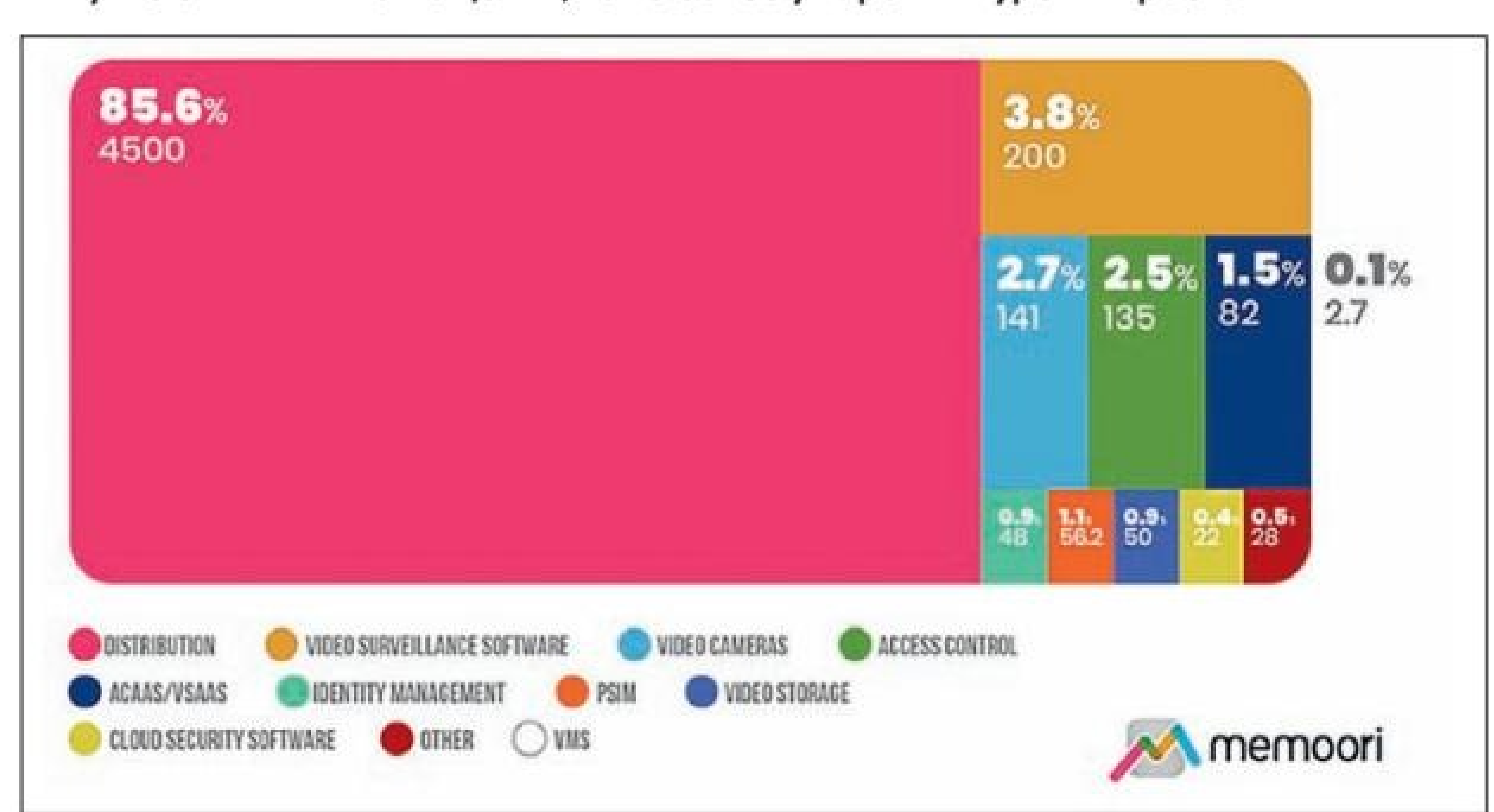
**В индустрии безопасности наблюдается снижение стоимости сделок по M&A (Mergers&Acquisitions, слияния и поглощения).
Memoori прогнозирует, что в ближайшие пять лет на рынке будет восстановлен импульс слияний и поглощений, но на более умеренных уровнях роста**

Данные о слияниях и поглощениях, собранные Memoori за последние 18 лет, показывают, что индустрия физической безопасности за это время прошла четыре цикла роста и спада.

Спады и подъемы

Ежегодный мировой отчет Memoori "Бизнес в области физической безопасности, 2020–2025 гг." показывает, что в 2019–2020 гг. (12-месячный период с октября 2019 г. по сентябрь 2020 г.) стоимость слияний и поглощений упала до 2,91 млрд долларов, что составляет сокращение примерно на 12% в сравнении с периодом 2018–2019 гг. Среднегодовая стоимость сделок M&A за последние 13 лет составила 6,71 млрд долларов, и Memoori полагает, что потребуется некоторое время, чтобы снова достичь этого уровня активности.

Несмотря на то что в последние 18 лет наблюдалась общая тенденция к росту консолидации, отрасль и раньше сталкивалась с волатильными изменениями в активности слияний и поглощений. В период с 2009 по 2011 г. после финансового кризиса 2008 г. в сфере безопасности произошла серьезная реструктуризация. Кроме того, примерно в этот период у крупных конгломератов (доход которых от ценных бумаг более 1 млрд долларов) отсутствовала уверенность и/или не было интереса вкладывать больше инвестиций в отрасль. В последнее время наблюдается нехватка покупателей из-за пределов бизнеса, особенно из сферы обороны и ИТ.



Слияния и поглощения на рынке систем безопасности, 2019–2020 гг., по секторам (% от общего количества сделок, количество сделок)

Основной движущей силой трансграничных слияний и поглощений всегда была необходимость расширения географического охвата, но в этом году стратегические приобретения были сосредоточены в основном на приобретении улучшенных технологических продуктов

Возможности средних компаний растут

Частный капитал (PE, или Private Equity) сохранил значительный интерес к индустрии физической безопасности, и в этом году PE-фирмы приобрели две охранные компании, инвестировав, однако, около 200 млн долларов – это скромная сумма по сравнению с предыдущими годами. Конкуренция усилилась, а норма прибыли упала в некоторых секторах бизнеса физической безопасности за последние три года, но в целом она показала хорошие результаты по сравнению с отраслью в целом. Есть еще много возможностей для консолидации, и потенциал роста бизнеса в следующие пять лет высок.

В течение последних семи лет открылось больше возможностей для средних специализированных компаний, ранее полностью зависевших от органического роста, для принятия стратегических приобретений для ускорения развития. Эти компании гораздо больше сосредоточены на каждом из трех секторов (контроль доступа, видеонаблюдение и охранная сигнализация/защита периметра), и это оказывает значительное и благотворное влияние на структуру рынка.

Структура отрасли по-прежнему очень фрагментированна: сотням небольших компаний становится все труднее конкурировать, и кажется неизбежным, что общая линия тренда стоимости и объема M&A восстановит свою динамику в течение следующих пяти лет, но при более скромном росте.

Частные фирмы всегда привлекал бизнес по обеспечению физической безопасности, и Memoori предполагает, что они имеют больше возможностей сейчас, когда пандемия идет на убыль. За последние два года около 150 новых стартапов внедрили программное обеспечение AI для предприятий видеонаблюдения и контроля доступа. Службы VSaaS и ACaaS должны укрепить свое финансовое положение, если они хотят удовлетворить растущий спрос на их услуги. Они быстро сжигают свои денежные средства от венчурных инвестиций, и IPO или SPAC могут быть выходом из этой ситуации.

В 2019–2020 гг. стоимость слияний и поглощений упала до 2,91 млрд долларов, что составляет сокращение примерно на 12% в сравнении с периодом 2018–2019 гг.

Межгосударственные сделки

На трансграничные приобретения приходилось 23% сделок, совершенных в этом году, по сравнению с 24% в 2018 г., 32% в 2017 г., 48% в 2016 г., 42% в 2015 г. и 50% в 2014 г. Основной движущей силой таких слияний и поглощений всегда была необходимость расширения географического охвата, но в этом году стратегические приобретения были сосредоточены в основном на приобретении улучшенных технологических продуктов и заполнении пробелов в решениях. Около 73% сделок были связаны с приобретением компаний США, подавляющее большинство которых были обусловлены внутренними обстоятельствами.

Заключение

Итак, период 2019–2020 гг. не был особенно позитивным для слияний и поглощений, но, учитывая, что отрасли пришлось справиться с пандемией, это неудивительно. В настоящее время отрасль более уверенно смотрит в будущее, и, похоже, нет недостатка в финансах для обеспечения будущих сделок. ■

По материалам www.securityinfowatch.com

Контрактная безопасность или безопасность как услуга?

Пользователи сегодня могут выбирать между компаниями, предоставляющими услуги контрактной безопасности ("обеспечение безопасности под ключ"), и поставщиками ACaaS и VSaaS нового поколения, которые сами являются производителями средств физической защиты и при этом стремятся продавать продукцию напрямую конечному пользователю



Оба подхода предоставляют комплекс услуг, которые снижают общую стоимость владения решением, заменяя разовые крупные платежи на небольшие ежемесячные, что очень актуально во время, когда пандемия опустошила карманы многих покупателей.

Контрактная безопасность

Бизнес контрактной безопасности существует более 40 лет, и в настоящее время в нем доминируют несколько крупных международных компаний, а также заняты сотни небольших местных операторов. Они покупают, устанавливают и используют различные технические решения и получают ежемесячную плату в обмен на гарантии обеспечения безопасности объектов по согласованным критериям и на основании сервисных договоров (SLA Agreement).

Новое поколение

Новое поколение поставщиков ACaaS и VSaaS, в основном из сферы производства средств физической безопасности, разработало свои продукты, основанные на собственных аппаратных и программных решениях в области видеонаблюдения и контроля доступа.

Ранее традиционный путь к рынку лежал через системных интеграторов и в некоторой степени сдерживал развитие и распространение ACaaS и VSaaS, поскольку интеграторы не заинтересованы в таком подходе. На сегодняшний день становится все более вероятным, что B2C-продажи будут расти как минимум в течение ближайших 10 лет. Безусловно, прямые продажи будут "конфликтовать" с более традиционными путями выхода на рынок, поэтому прогнозирование в этой сфере достаточно сложное.

К сожалению, существует мало открытых источников информации по рыночным данным касательно VSaaS. По наиболее позитивным оценкам аналитиков Memoori, мировые продажи VSaaS в 2019 г. составили около 1,6 млрд долларов, что включает стоимость оборудования и программного обеспечения по розничным ценам вместе с относительно небольшой долей дохода от подписок. Выручка "контрактной безопасности" только в США, включая обеспечение безопасности с участием команды охранников, оценивалась в 28 млрд долларов в 2020 г., из которых 2 млрд долларов составляли доходы от электроники и системной интеграции.

Производители переходят на прямые продажи

Вендоры из сферы физической безопасности запускают сценарий выхода на розничные рынки и начинают продавать решения ACaaS и VSaaS напрямую клиенту и/или предлагать оплачиваемый на ежемесячной основе пакет услуг, за который вносится аванс.

Это делает рынок более конкурентным: компании, фокусирующиеся на комплексной контрактной безопасности, будут расширяться за счет поглощения, а вендоры средств физической защиты покажут органический рост в сегменте продуктов ACaaS и VSaaS.

Ежегодный доклад Memoori "Бизнес в сфере физической безопасности с 2020 по 2025 г." показал, что спрос на VSaaS вырос во втором и третьем кварталах 2020 г. на фоне роста на 10% в 2019 г. Учитывая проблемы, вызванные пандемией, это очень уверенный рост, и аналитики прогнозируют, что к 2025 г. рынок может достичь объема 2,6 млрд долларов. ■

По материалам www.memoori.com

К 2024 году рынок ACaaS вырастет до 1,6 млрд долларов

По оценкам исследователей, в 2019 г. инвестиции в ACaaS (Access Control as a Service, контроль доступа как услуга) составили 620 млн долларов, из которых примерно 40% были сделаны в Северной Америке. Ожидается, что к 2024 г. спрос на услугу вырастет до 1,6 млрд долларов. По сведениям Memoori World Market, многие организации в настоящее время изучают, как они могут использовать облако, поскольку это оказывается очень привлекательным предложением

Аналитики обнаружили, что по мере того, как устанавливается все больше IP-СКУД (систем контроля и управления доступом), а технологии, связанные с проверкой личности, расширяют свое проникновение, использование ACaaS и управляемых услуг становится все более привлекательным для конечных пользователей, особенно тех, кто уже привык к корпоративным облачным сервисам.

Благодаря ACaaS у конечных пользователей отпадает необходимость в масштабных ИТ-отделах для создания и обслуживания серверов и инфраструктуры в бизнес-центре, что требует больших первоначальных капитальных затрат. При использовании облачных решений локальные серверы и устройства исключаются; исследования показывают, что это должно снизить общую стоимость владения СКУД без потери функциональности. По мнению аналитиков, переход на облачные сервисы также сделает более легкой интеграцию контроля доступа с корпоративными системами, такими как управление идентификацией и доступом (IAM), что повысит их ценность.

ACaaS проникла в сектор малых и средних зданий, где арендаторы предпочитают регулярную ежемесячную арендную плату, а не единовременную выплату, которая включает техническое обслуживание оборудования и программного обеспечения. Существующие владельцы систем видеонаблюдения и контроля доступа, которым необходимо модернизировать свою деятельность, будут все чаще приглядываться к варианту "контроль доступа как услуга".

COVID-19 за последние двенадцать месяцев истощил финансовые ресурсы многих конечных пользователей СКУД, что сделало сокращение первоначальных затрат еще более привлекательным.

Управление доступом традиционно осуществлялось через системных интеграторов, и хотя они постепенно убеждаются в неизбежности роста ACaaS, процесс массового внедрения облачных технологий займет некоторое время. ■

По материалам www.securityworldmarket.com

Критические факторы, которые обеспечат рост физической безопасности к 2025 году

Что обеспечивает будущее индустрии физической безопасности в следующие пять лет? Рынку требуются фундаментальные изменения в бизнес-стратегиях



Разрыв между компаниями увеличивается

Дистанция между основными поставщиками оборудования для видеонаблюдения и многими сотнями более мелких поставщиков увеличивается с каждым годом, высота минимального экономического порога для работы "в плюс" для новичков рынка растет очень быстро.

Китай в настоящее время фактически является закрытым для некитайских товаров рынком, на который приходится не менее 40% мирового потребления, и большую часть этого рынка контролируют всего две китайские компании. Эти фирмы ранее инициировали "гонку ко дну", которая нанесла значительный ущерб сотням малых и средних компаний по всему миру.

Бизнесу видеонаблюдения требуется новая стратегия, ориентированная либо на объем через рынок малого и среднего бизнеса (SMB), либо на бренд через корпоративный бизнес.

Слияние и поглощение ведущих западных производителей рассматривается как возможное решение для соразмерного соперничества с Hikvision и Dahua, но в лучшем случае это может только замедлить дальнейшее увеличение разрыва. Сильные бренды с комплексными решениями, которые, возможно, ориентированы на ряд вертикальных рынков, и наличие прочных альянсов с компаниями, занимающимися другими услугами по автоматизации зданий, – это еще один вариант для поставщиков оборудования, обеспечивающий прибыльное будущее.

Киберзащита – залог успеха

Парадоксально, но оборудование физической безопасности, которое обеспечивает безопасность людей и имущества в зданиях и общественных местах, часто имеет высокий уровень риска кибератак.

Поставщики, которые смогут подтвердить хорошую защищенность своей продукции от киберпреступлений, получат больше корпоративных покупателей. Те, кто продает уязвимые продукты, в лучшем случае обнаружат, что их доля на рынке снизится, и, вероятно, они столкнутся с финансовыми убытками, которые могут разрушить их бизнес. Производители средств физической защиты должны принимать все возможные меры для минимизации угроз кибербезопасности. Чем больше услуги отрасли интегрируются с другими услугами в IP-сетях, тем выше вероятность киберугроз.

Искусственный интеллект

В 2020 г. видеоаналитика ИИ стала мейнстримом, но прогнозируемый рост все еще является для нее определенной проблемой. Развитие программного обеспечения с искусственным интеллектом продолжится, базируясь на огромных объемах информации, которая генерируется датчиками оборудования физической безопасности, в частности видеокамер.

Существует очень большой рынок для применения ИИ-видеоаналитики в существующих реалиях, искусственный интеллект меняет правила игры и окажет серьезное влияние на бизнес видеонаблюдения.

Производители средств физической защиты должны принимать все возможные меры для минимизации угроз кибербезопасности. Чем больше услуги отрасли интегрируются с другими услугами в IP-сетях, тем выше вероятность киберугроз

Интеграция с IoT и BIoT

Интеграция ИТ-систем в тренде уже более 10 лет, но только за последние три года благодаря IP-сетям и открытым стандартам начали появляться более элегантные и недорогие эффективные решения.

Теперь интеграция дошла до IoT и Building Internet of Things (BIoT), которые объединяют все службы автоматизации в зданиях и сооружениях. Сегодня мы можем создавать передовые интегрированные системы безопасности, предназначенные для обеспечения контроля всех точек, генерирующих данные, что позволяет персоналу службы безопасности быстро находить различную информацию и анализировать ее.

SaaS

Облачным сервисам VSaaS и ACaaS потребовалось около 10 лет, чтобы утвердиться в сфере профессионального видеонаблюдения и контроля доступа. За последние два года к ведущим поставщикам присоединились 34 компании.

Спрос значительно вырос за последние два года, и, по прогнозам аналитиков, в следующие пять лет он будет показывать среднегодовой темп роста примерно 12%. Остается только один беспокоящий момент: ваш видеоархив находится в общедоступном облаке (AWS, Azure и т.д.), то есть фактически у вас нет прямого контроля за ним. Для некоторых секторов, например финансового, это является критичным моментом. Скорее всего, крупные игроки примут стратегию развертывания частных облаков.

При этом такие компании, как Amazon, Google и Microsoft, инвестируют миллиарды долларов в облачные сервисы. Эти компании теперь могут не только предоставлять клиентам вычислительные мощности с оплатой по факту использования, но также и анализировать информацию с помощью программного обеспечения с ИИ, предоставляя действительно ценные аналитические данные.

Коронавирус

COVID-19 открыл новые возможности для бизнеса в области физической безопасности. Будет внедряться все больше инновационных продуктов и систем, они станут играть существенную роль в борьбе с вредоносными вирусами, если таковые появятся в течение следующих нескольких десятилетий.

Вакцины спасают жизни, но это не единственное решение. Нам нужно быть намного лучше подготовленными к борьбе с распространением вирусов типа COVID-19, и системы физической безопасности могут внести значительный вклад в обеспечение сохранности жизни и здоровья населения. ■

По материалам www.asmag.com

Подсчет людей: LiDAR против камеры

В последние годы подсчет количества людей играет все большую роль в самых различных сферах, огромный интерес к нему проявляет бизнес. Данные, полученные от систем учета посетителей/клиентов, находят самое широкое применение у компаний и предприятий из разных областей экономики и разного профиля

Подсчет людей стал критически важной потребностью для бизнеса. Различные исследовательские агентства прогнозируют, что рынок решений для подсчета посетителей будет расти уверенными темпами до 10% в год в течение следующих 4–5 лет.

Системы подсчета людей на основе камер видеонаблюдения, использующие возможности аналитики, стали в последние годы популярным выбором. Но, с другой стороны, решения, использующие технологию LiDAR, дают определенные уникальные преимущества. Ниже – коротко о плюсах каждой технологии.

Преимущества подсчета людей на основе LiDAR

1. Простота использования на открытом воздухе. Освещение и тени не влияют на качество работы.

2. 3D-детекция: лучшее покрытие, чем у большинства сенсоров, таких как датчики пересечения луча, на входе/выходе в дверях.

2. Для выполнения видеоаналитики решения LiDAR не требуют обработки алгоритмов компьютерного зрения высокопроизводительным графическим процессором, они предлагают привлекательное ПО.

3. В отличие от камер, которые необходимо устанавливать над головами людей в местах входа/выхода, решения LiDAR обладают большей гибкостью в плане выбора места установки.

Преимущества подсчета людей с помощью камеры

1. Возможность лучше идентифицировать людей, идущих близко друг к другу, и лучше определять слоняющихся в зоне подсчета, тем самым обеспечивая более высокую точность результатов.

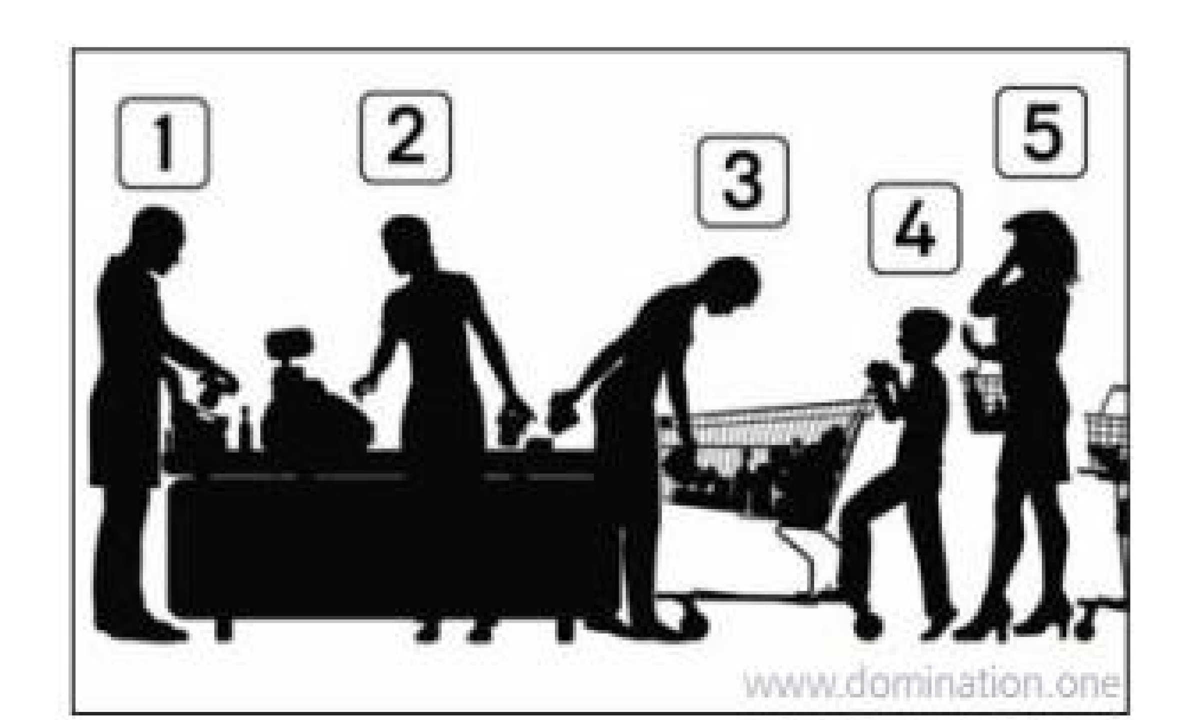
2. Возможность проверки результата: счетчики на базе камеры дают возможность проверить точность подсчета в видеоархиве и произвести дополнительные настройки. У систем без камер такой возможности нет.

Ограничения

Как LiDAR, так и решения для подсчета людей на основе камер имеют свои ограничения. Проблема любой системы подсчета состоит в том, чтобы отличить людей от других объектов, например тележек для покупок, детских колясок, животных или теней на полу, и правильно идентифицировать идущих близко друг к другу, идущих очень быстро или несущих большие предметы.

Использование камер для подсчета людей дает лучшие возможности для управления проблемными ситуациями. Технология стереокамер и современные алгоритмы на основе искусственного интеллекта, обученные с использованием соответствующих видеоматериалов, еще больше повышают точность подсчета.

Часто возникает необходимость отдельно вести учет взрослых и детей, а также отделить персонал от клиентов. Опять же, технология стереокамеры в сочетании с хорошо обученными алгоритмами на основе искусственного интеллекта – это метод, идеально подходящий для



правильной идентификации взрослых и детей. Наличие у сотрудников специальных значков, спецодежды или RFID-меток помогает отличать их от клиентов и посетителей.

Заключение

Как было сказано выше, и LiDAR, и системы подсчета людей на основе камер имеют свои преимущества и недостатки. Окончательное решение о выборе технологии будет зависеть от многих факторов, в том числе от характера местоположения, бюджета, вычислительной мощности и т.д. Рынок постоянно растет, и в ближайшие годы мы сможем увидеть больше технологических разработок в этой области. ■

По материалам www.asmag.com

Новости ONVIF

Развитие сферы IP-продукции для обеспечения безопасности, возрастающая потребность в интеграции устройств разных производителей заставляют специалистов отрасли активно искать решение проблемы их совместимости и работать над созданием единых стандартов и протоколов

ONVIF – это глобальная инициатива по стандартизации продуктов физической безопасности на основе IP.

GitHub

В прошлом году ONVIF развернула платформу на GitHub. Переход на популярную платформу для разработки ПО с открытым кодом – это значительный шаг к ускорению процесса разработки и сокращению времени между релизами.

Profile M

ONVIF анонсировала релиз-кандидат для Profile M, который поддерживает конфигурацию аналитики и информационный запрос для метаданных, а также фильтрацию и потоковую передачу метаданных. ONVIF Profile M открывает возможность извлечения данных, которые не только имеют ценность для приложений безопасности, но и могут использоваться в промышленности для других целей.

Профили ONVIF для 20 000 устройств

Более 20 тыс. продуктов безопасности теперь соответствуют различным профилям ONVIF. Это свидетельствует о высоком рыночном спросе на функциональную совместимость аппаратного и программного обеспечения и подчеркивает значение ONVIF как лидера разработки открытых стандартов в области физической безопасности.

Значительный рост количества совместимых продуктов ONVIF произошел в последние несколько лет: в 2018 г. их число превысило 10 тыс. единиц. Ожидается, что готовящийся к выпуску Profile M для метаданных будет стимулировать дальнейший рост числа таких продуктов для удовлетворения потребностей в совместимости в облачных решениях и системах с расширенной аналитикой на базе искусственного интеллекта.

Адаптироваться к меняющемуся ландшафту

Безопасность претерпевает коренные изменения. Индустрия эволюционировала от простого видеонаблюдения к использованию ИИ и Интернета вещей для достижения различных целей безопасности и бизнеса. Использование ИИ напрямую связано с комбинированием данных камер и данных с различных датчиков. Задача ONVIF – обеспечить совместимость, которая стала важнее, чем когда-либо. Пандемия показала, насколько конечным пользователям важны решения, объединяющие устройства разных производителей. Безусловно, ONVIF будет и дальше адаптироваться к меняющемуся ландшафту индустрии безопасности и глобальным требованиям. ■

По материалам www.securityworldmarket.com и www.asmag.com

Автомобильные камеры со встроенными радарами

Автопромышленность продолжает развиваться бурными темпами, при этом все больше внимания уделяется различным аспектам безопасности. Для решения соответствующих проблем уже давно используются автомобильные камеры, теперь они получили такой действенный инструмент, как радар

Согласно новому отчету аналитического агентства Marketsandmarkets, объем мирового рынка автомобильных камер с интегрированными радарами вырастет с 6,1 млрд долларов в 2021 г. до 10,1 млрд к 2026 г.

Этот сектор будет расти со среднегодовым темпом 10,5% с 2021 по 2026 г. Увеличивающийся спрос на передовые системы безопасности транспортных средств для автомобилей премиум-сегмента и усиление требований к безопасности в транспортных средствах являются основными драйверами роста.

Модуль "камера + радар" в автомобиле может использоваться с различными целями, это адаптивный круиз-контроль (Adaptive Cruise Control), предупреждение о возможности лобового столкновения (FCW), смягчение или предотвращение столкновений с помощью автоматического торможения и системы предупреждения о сходе с полосы (LDW). Интеграция камеры и радара в единый модуль приводит к совокупному снижению стоимости устройства, так как используется общая электроника.

ADAS – основной драйвер

Ожидается, что с ростом внедрения усовершенствованной системы помощи водителю (ADAS) рынок интегрированных с радарами камер в ближайшие годы значительно увеличится. В 2021 г. наибольшим спросом будут пользоваться решения для фронтального обзора, и предполагается, что эта тенденция сохранится до 2026 г. ADAS помогает следить за движением транспортного средства, чтобы автомобиль мог поддерживать безопасную и разрешенную скорость, оставаться на своей полосе, сохранять дистанцию между собой и движущимися впереди машинами и реагировать на чрезвычайные ситуации. Фронтальные камеры ADAS улучшают функции активной безопасности и помощи водителю, такие как автономное экстренное торможение, адаптивный круиз-контроль, система помощи при удержании полосы движения и помощь в пробке. Развитие ADAS активно поощряется на правительственном уровне.

Широкое распространение рейтингов безопасности транспортных средств и снижение стоимости компонентов будут способствовать развитию рынка автомобильных камер с интегрированными радарами.

Европа занимает наибольшую долю рынка

Европа заняла наибольшую долю этого рынка в 2020 г., прежде всего за счет собственных технологических разработок, повышенного спроса в регионе на максимально безопасные автомобили и наличие сильной автомобильной промышленности.

Bosch, Aptiv, ZF Friedrichshafen, Continenta, Valeo, Magna, Veoneer, Nidec, Intel и Infineon – это лишь некоторые из основных игроков на рынке автомобильных камер с интегрированными радарами, упомянутых в отчете Marketsandmarkets. ■

По материалам www.securityworldmarket.com

Приоритеты государств: ускоренное внедрение технологий безопасности и идентификации граждан

Интерес и повышенное внимание со стороны правительств к тем или иным технологиям, актуальным на сегодняшний день либо имеющим перспективы широкого применения в будущем, во многом определяет их темпы развития и масштабы внедрения

Исследовательское агентство Gartner назвало основные тенденции технологий 2021 г., которые могут ускорить инновации в ИТ и оптимизировать либо преобразовать государственные услуги.

Эти тенденции обусловлены проблемами, вызванными пандемией, и необходимостью создания гибких моделей операционной деятельности, с учетом возможных сбоев и чрезвычайных ситуаций.

Пандемия COVID-19 стимулировала ускорение внедрения цифровых инноваций в госсекторе по всему миру. Благодаря им у государства появились новые возможности для укрепления доверия граждан и повышения гибкости деятельности соответствующих учреждений.

Адаптивная безопасность

Адаптивный подход к безопасности рассматривает риски, доверие и безопасность как часть непрерывного процесса, в ходе которого возможно предвидеть и смягчать постоянно возникающие киберугрозы. Этот подход включает компоненты для прогнозирования, предотвращения, обнаружения и реагирования на угрозы. Адаптивная безопасность отходит от традиционных представлений о периметре, предполагая, что нет границ между безопасным и небезопасным, – это является необходимым концептуальным сдвигом с учетом перехода к облачным сервисам.

Агентство Gartner прогнозирует, что к 2025 г. 75% ИТ-директоров госорганизаций будут нести прямую ответственность за безопасность за пределами ИТ.

Всё как услуга (XaaS)

XaaS – это облачная стратегия поиска поставщиков, в которую входит приобретение всего спектра бизнес- и ИТ-услуг по подписке. Реагирование на пандемию и острая потребность в цифровых услугах усугубили необходимость модернизации приложений и инфраструктуры. XaaS предлагает альтернативу модернизации устаревшей инфраструктуры, обеспечивает масштабируемость и сокращает время на предоставление цифровых услуг.

Прогнозируется, что к 2025 г. 95% новых инвестиций в ИТ, сделанных государственными учреждениями, будут осуществляться в виде сервисного решения.

Цифровая идентичность гражданина

Цифровая идентификация гражданина – это возможность подтвердить личность человека через государственные цифровые каналы для подключения и получения доступа к государственным услугам.

Gartner прогнозирует, что к 2024 г. на рынке появится настоящий глобальный децентрализованный стандарт идентификации, который будет учитывать деловые, личные, социальные варианты использования.

Гражданская активность

Прямое участие граждан в муниципальном и государственном управлении достигло новых высот в 2020 г., поскольку много людей, проживающих в одном районе, муниципальном образовании и т.д., сообща боролись с пандемией, лесными пожарами, ураганами и другими бедствиями.

По прогнозам, как минимум треть стран будут использовать цифровые показатели вовлеченности для отслеживания количества и качества участия граждан в принятии политических и касающихся бюджета решений к 2024 г.

Оперативная аналитика

Gartner прогнозирует, что к 2024 г. 60% государственных инвестиций в ИИ и аналитику данных будут направлены на организацию сбора данных и оказание непосредственного влияния на оперативные решения и результаты в реальном времени. ■

По материалам www.securityworldmarket.com

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Виктория Козлова
Руководитель направления исследования перспективных технологий Дирекции по инновационному развитию и партнерству компании "Тандер" (розничная сеть "Магнит")

Биометрия в ритейле: как не подорваться на "мине" и получить устойчивые эффекты

Ритейл – отрасль, которая активно внедряет биометрические системы для решения самых разных задач – привлечения новых покупателей и повышения лояльности, сбора и анализа данных для таргетированного взаимодействия с клиентом, учета рабочего времени сотрудников, усиления безопасности и т.д. Внимание компаний обращено на технологичные и быстро интегрируемые решения, которые позволят в измеряемые сроки увидеть реальные эффекты и пользу для бизнеса. Виктория Козлова из компании "Тандер" (розничная сеть "Магнит") рассказала о бизнес-эффектах, которые уже сегодня можно достичь с помощью биометрических технологий, основных подводных камнях, с которыми сталкиваются компании на этапе внедрения и эксплуатации, и перспективами биометрии на глобальном уровне



– Какие меры нужно предпринять, чтобы пользователи доверяли биометрическим технологиям?

– В каждом кейсе с биометрией есть свои нюансы, но общее скорее в следующем.

Да, биометрии не доверяют, потому что не знают. Если обеспечить должное знакомство – объяснить, какие используются средства, как используется информация и прочее, и, конечно, на доступном языке, – это уже большой шаг в сторону популяризации.

Второй вопрос – должно быть удобно и выгодно конечному пользователю. Без этого технология будет восприниматься как навязанное средство контроля со стороны государства, существующее для всевозможных заговоров против человечества.

Люди боятся слежки и не уверены в защите данных. Есть категория пользователей, которые даже не могут объяснить, чего именно опасаются...

По факту реальные угрозы лежат в области защиты информации: атаки при предъявлении ID и атаки на утечку данных. Мы знаем, что модели угроз здесь уже созданы и находятся в процессе улучшений на стороне разработчиков и государства. Нормативно-правовая документация в некотором объеме уже составлена и находится на этапе утверждения, после чего появится зеленый свет для более интенсивного распространения технологии в РФ. Разработка всеобъемлющих регулирующих процедур позволит объяснить людям правовые моменты в эксплуатации биометрического ID, улучшится понимание, как себя вести, что делать в разных случаях, то есть границы правового поля станут четче. В общем, когда туман рассеется, появится больше доверия.

– Созрели ли общество, ритейл для внедрения таких решений?

– Конечно. Общество стало зреть в том момент, когда начало активно использовать Face ID в смартфонах. Биометрия уже стала технологией повседневного и бытового применения. Как вы знаете, рынок мобильных устройств огромен, и ее распространение посредством телефонов начиналось сразу стремительно и масштабно. Это, кстати, очень естественный и самый ненасильственный подход, когда такая, казалось бы, достаточно охранная по своей сути технология спустилась на пользователей не как "обязалово" со стороны государства, а как полезная утилита, к уровню комфорта которой начала вырабатываться привычка сначала на бытовом уровне, а затем стало появляться доверие в ряде других сфер...

А если мы говорим о ритейл-компаниях, то здесь уже успели оценить ценность и сформулировать бизнес-кейсы, начиная от контроля доступа и заканчивая платежными сервисами. Мы с коллегами по ритейлу видим массу положительных откликов от покупателей, например, по платежам. Самые частые комментарии – "прикольно и быстро", "экономите мне заряд телефона"; поступают и инициативы вроде "сделайте так, чтобы к моей карте можно было привязать Face ID детей и поставить ограничение на товары и сумму в день"... Конечно, есть и отрицательные отзывы: "не хочу, чтобы за мной следили", "я знаю, вы отдадите мой шаблон другим компаниям", "а вдруг похожий на меня человек снимет деньги с моей карты" и др.

Но все эти опасения идут от недостаточного опыта использования и со временем будут сходить на нет, особенно принимая во внимание темпы роста рынка биометрии.

– Каких эффектов ритейл ждет от биометрии?

– Обычно выделяют три статьи эффективности, по которым окупаемость должна быть менее двух лет: издержки, потери и продажи (то есть прямой доход).

Кейсы, например, по контролю доступа (физическому или виртуальному) связаны со снижением рисков и могут предотвращать потери (вынос товара или злоупотребление информацией на рабочем ПК) и сокращать издержки (замена имеющихся более устаревших систем, когда дешевле купить новую СКУД вместо того, чтобы актуализировать старую, либо старая уже вовсе перестала отвечать современным задачам). Иногда компания просто принимает волевое решение о переходе на новую систему как на новый стандарт качества, чтобы соответствовать новым бизнес-процессам, и готова инвестировать, понимая, что это не вклад с прямой доходностью, а необходимое средство для работоспособности смежных процессов, уже имеющих прямое влияние на продажи. Например, в случае с биометрической СКУД или системой учета рабочего времени понадобится минимум полгода, чтобы ощутить на бизнесе более-менее устойчивые эффекты улучшений.

Кейсы с более прямой доходностью – платежи и Face ID для программ лояльности, где рост NPS

(Net Promoter Score, индекс потребительской лояльности) влечет за собой рост продаж посредством привлечения либо возвращения/удержания трафика. И здесь пора говорить о том, что технология достаточно скоро мигрирует в статус неотъемлемого платежного сервиса. Поэтому если у тебя на кассе не будет сервиса, к которому привык покупатель в других сферах, то к тебе он может потом и не вернуться...

Для таких кейсов достаточно замеров от трех месяцев использования при условии, что технологию разместили в правильной локации, где публика предварительно разогрета биометрией. То есть это город-миллионник, возрастной диапазон – до 35 лет, высокотрафиковый район города, где процент безналичных платежей – от 80% и др. Важным критерием успешности является удобная встройка в процесс обслуживания, в том числе формфактор устройств. К примеру, биометрия хорошо дополняет и финализирует сервисы самообслуживания, хотя в некотором будущем представляется, что большая часть приема платежей не будет иметь как такового физического представления в магазине, будут сокращаться кассы с кассирами и самообслуживание перейдет на мобильное устройство, так как общая тенденция развития ритейла неумолимо идет к автоматизации всего и вся. А магазины с живым обслуживанием останутся уникальными фичами, куда вы приходите больше за опытом, нежели за покупкой...

– Кто в крупных компаниях должен быть внутренним заказчиком внедрения биометрических технологий, чтобы проект состоялся?

– Смотря какой кейс. Если учет рабочего времени, минимальный состав – это департаменты персонала, операций/продаж, ИТ и, может быть, департамент экономической безопасности. Если контроль доступа – департаменты экономической безопасности, персонала, ИТ и операций/продаж.

Если платежи и лояльность (а эти два кейса оптимальнее вести вместе, так как один следует из другого), то внутренними заказчиками будут отдел маркетинга, финансовый департамент, ИТ и департамент операций/продаж, так как именно они проводники технологии на местах.

– С какими барьерами внедрения биометрии ритейл встречается чаще всего?

– На старте трудно сложить кейс и экономику, чтобы все билось. Если у вас это получилось, вы проходите в следующий раунд. Здесь лучше задержаться и не жалеть времени на должный анализ, чтобы потом не было недоразумений и "неожиданного" прекращения проекта. Для этого нужно, чтобы в команде проекта были правильные люди, непосредственные бенефициары технологии, чтобы сложилась картинка взаимовыгод всех участников и общее видение, куда идем. Важно также разложить этапы с пониманием, на каком из них какого эффекта можно достичь, так как частая "мина", на которой все подрываются, – это когда бизнес-заказчик хочет все и сразу, если не видит магии после первого месяца использования, говорит, что технология не работает или не выполняются KPI...

В ходе самого теста конечные пользователи часто его боятся, не доверяют, о чем мы уже говорили выше. Или просто решают саботировать внедрение (например, сотрудники, если речь об учете или контроле). Нужно правильное донесение, реклама, обучение, чтобы весь путь от сдачи до использования биометрии был удобнее и быстрее любого текущего процесса, чтобы он был безопасен, чтобы была польза и благо от применения. Другими словами, нужна правильная мотивация и вовлечение в пилот тех, кто в дальнейшем будет главными действующими лицами.

При внедрении предстоит некоторая интеграция в архитектуру корпоративных систем, и здесь важно провести соответствующее проектирование для учета всех требований бизнеса и корректной передачи данных от и к оператору биометрической системы, чтобы этот этап не стал стопором в рамках масштабирования.

– Ваше видение – каким станет общество при длительном использовании биометрических решений?

– Абсолютная тенденция на сокращение посредничества, появление больших возможностей у получателей услуг. Все идет к тому, что у человека становится меньше девайсов/токенов в принципе, и основным связующим их звеном будет биометрия. Люди станут максимально автономны как внутри своей страны, так и за ее пределами.

Со стороны государства будут поддерживаться юзкейсы в рамках различных госпрограмм – пенсионные начисления/выплаты, медобслуживание, электронные паспорта и другие ID, выборы, налоги, штрафы, кейсы с физическим и виртуальным доступом куда бы то ни было.

В итоге автоучет биометрических ID ожидается в большом количестве систем, которые будут присутствовать в некотором виде в магазинах, учебных заведениях, банках, на заправках, МВД, транспорте и т.д. Документы как физические носители исчезнут. Биометрические системы будут объединяться друг с другом и взаимодействовать. Сейчас уже тестируются социальные рейтинги среди населения, основанные на истории всего того, что происходило с человеком. Это работает в Китае в виде личного рейтинга гражданина: каждого оценивают по параметрам из систем массового наблюдения. У человека копится история поведения и событий, в которых он участвовал, эти события подлежат оценке, на основе которой с ним ведут себя определенным образом, и он может рассчитывать на определенные блага. Достаточно футуристичная и концептуальная история, трудно пока судить, когда она придет к нам...

Бесспорно, биометрическая технология имеет огромные возможности для улучшения жизни людей в целом. К сожалению, эти возможности связаны также со злоупотреблениями, многие из них крутятся в этическом поле, и в основном вокруг конфиденциальности и фрода. Любое нововведение вызывает ответную реакцию у общества, порождая массу идей по новым способам его использования и "обхода". Идентификация людей может привести к возникновению таких проблем, как групповая дискриминация (по половому, этническому, возрастному и другим признакам), стать инструментом банковского и коммерческого мошенничества, а может быть и креативным оружием. Например, еще в 2015 г. в Гонконге группа энтузиастов воссоздала по ДНК внешность людей, которые бросали мусор на улице. Они целенаправленно ходили и собирали биоматериал, а затем транслировали изображения этих людей на экранах в общественных местах (метро, вокзалы) со словами, что есть "вот какие негодяи" и не нужно делать, как они. И это имело свой эффект.

Очевидно одно: с появлением каждой новой технологии общество немного условно "мутирует", ассимилирует... И категорично говорить о том, плохо это или нет, наверное, неправильно. ■

"Магнит" начал внедрять в магазинах оплату взглядом

Новый способ оплаты одним взглядом уже доступен в десяти магазинах ПАО "Магнит" в Москве, Краснодаре и Ростове-на-Дону. Компания планирует к июню подключить к сервису более 100 торговых точек в Москве и Краснодаре.

Сервис оплаты одним взглядом внедряется совместно со Сбербанком. Он работает на планшете с 3D-камерой, которая за счет высокой точности распознавания и захвата глубины легко считывает черты и изгиб лица с учетом изменений во внешности. Банк обеспечивает максимальную безопасность, а также исключает взлом и подмену биометрических данных за счет постоянного улучшения методов распознавания.

Чтобы воспользоваться новой технологией, необходимо быть клиентом банка и заранее в отделении или в мобильном приложении "Сбербанк Онлайн" активировать распознавание по лицу и указать карту, с которой будут списываться средства. На кассе в магазинах "Магнит", где тестируется технология, на дисплее пин-пада достаточно выбрать кнопку "Оплатить одним взглядом" и взглянуть на планшет. Других действий не требуется.

"Новая технология позволяет с легкостью приобрести товары без наличных денег, карты или телефона. Предварительные результаты показывают, что процесс оплаты покупок ускорился в несколько раз. Хронометраж процесса показывает, что вместо 34 секунд при оплате наличными и 15 секунд при безналичной оплате теперь тратится всего 3 секунды. Решение о масштабировании мы будем принимать, когда изучим отклик покупателей и потенциальное влияние сервиса на бизнес-показатели", – прокомментировал Эдуард Ирышков, директор департамента розничных технологий сети "Магнит".

Источник: www.magnit.com

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Марат Садеков
Руководитель направления проектов Business Continuity Management X5 Retail Group

SOA для проектного управления. С оркестром!

Успешный опыт X5 Retail Group

Видели ли вы проекты, для которых недостаточно одного менеджера? Надо назначить еще одного... Или лучше двух... В помощь первому – проект ведь "очень большой". Финал у таких историй предсказуем, так как менеджер у проекта должен быть один – для меня это аксиома. Как обеспечить разумную загрузку менеджера проекта и не создать очередную "лебедь-рако-щуку"? Как применить индивидуальный подход к группам специалистов, участвующих в решении масштабной многоплановой активности (свои сотрудники и подрядчики, консультанты SAP и тестировщики, спецы по инфраструктуре и портальщики)? Как увязать задачи, подлежащие четкому планированию, и исследовательские задачи, требующие гибкого подхода? Как увязать расписание этих задач с операционной деятельностью компании? Попробуйте реализовать управление через программу проектов

С конца нулевых, чуть более 10 лет, компания X5 Retail Group (X5) эксплуатировала дата-центры как на территории России, так и за рубежом. Большое количество критичных систем было размещено в дата-центре IBM в Швейцарии. С 2015 г. в связи с новыми требованиями законодательства РФ, а также изменениями экономической ситуации и стремлением минимизировать валютные риски компания начала сокращать размещение информационных систем в европейском ЦОД.

В 2018 г. в X5 было принято решение о переносе оставшейся части информационных систем из европейского ЦОД (ЕЦОД), в ЦОД на территории РФ (РосЦОД). Тот факт, что в 2019 г. заканчивался очередной цикл эксплуатации большей части ИТ-инфраструктуры систем в ЕЦОД (необходимость увеличения производительности в связи с органическим ростом числа магазинов торговых сетей и истечение сроков вендорской поддержки), жестко ограничивал сроки миграции I кварталом 2020 г.

Подготовка к масштабной миграции

На момент, когда принималось решение о миграции, ландшафт систем, размещенных в дата-центре в Женеве, примерно соответствовал представленному на рис. 1.

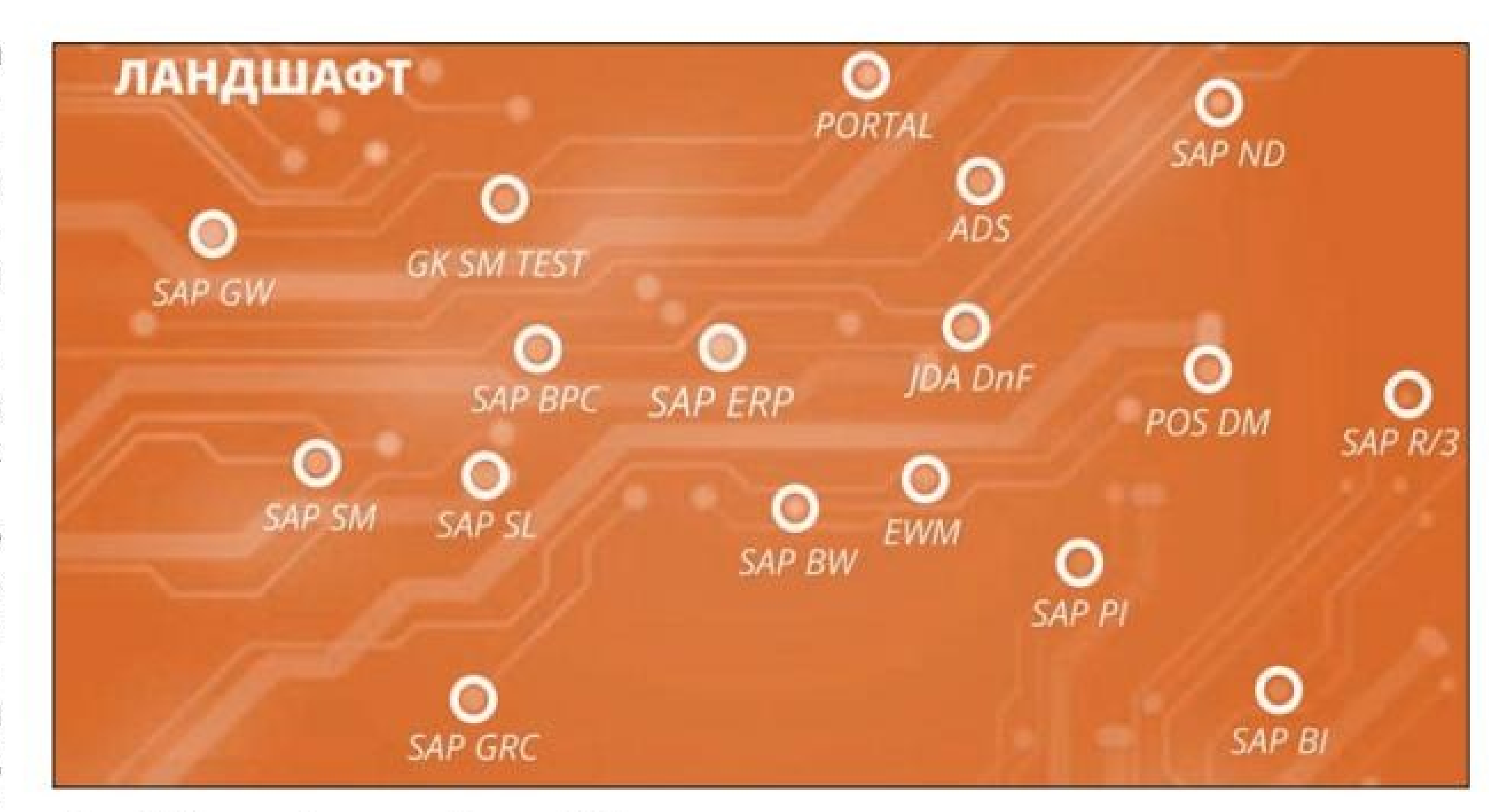


Рис. 1. Ландшафт европейского ЦОД

Ключевой системой являлась SAP ERP – одна из крупнейших инсталляций в мире. Помимо SAP ERP, в ЕЦОД функционировали системы, автоматизирующие процессы пополнения и товародвижения в магазинах, интеграционная шина и ряд других критичных для бизнеса систем (High Load). Требовалось исключить риски сбоев в работе этих систем как во время, так и после их миграции, поскольку от их стабильной работы зависит то, как "бьются" чеки в 17 тыс. магазинов X5 по всей стране.

Перед миграцией систем в РосЦОД был установлен, протестирован и введен в эксплуатацию комплекс технических средств (18 стоек), создающих запас производительности до 2022 г. включительно. Для того чтобы обеспечить надежный процесс репликации между площадками (ЕЦОД и РосЦОД), были организованы два дополнительных временных канала связи. Были также разработаны и одобрены документы, описывающие порядок миграции систем, согласованные плановые и резервные окна DT, порядок тестирования и сроки стабилизации после миграции. Параллельно с этим решались задачи создания и ввода в эксплуатацию георaспределенного кластера интеграционной шины (ГРК SAP PO) на территории РФ, обновления версии интеграционной шины, переключения интеграционных потоков из ЕЦОД на ГРК SAP PO в РосЦОД, подготовки к выводу из эксплуатации, утилизации и продаже оборудования в ЕЦОД по мере его высвобождения.

В то же время технические владельцы информационных систем работали над сокращением требований к инфраструктурным мощностям, актуализацией описаний интеграционных потоков и сокращением списка интеграций (по итогам миграции до 300 интеграционных потоков были выведены из эксплуатации как потерявшие актуальность).

Выбор подхода к управлению

Традиционным для нас, как и для большинства ИТ-служб в РФ, подходом к решению перечисленных выше задач было создание временной организационной структуры в виде одного крупного проекта. Чтобы избежать классических проблем, свойственных всем "мегапроектам", я предложил руководству реализовать управление через формирование программы проектов. По аналогии с SOA (англ. Service-Oriented Architecture) модульный подход к реализации изменений в компании дает определенную гибкость в управлении. Каждый из проектов программы решал одну из крупных задач либо минимизировал риски, обусловленные реализацией "головного" проекта, который, в свою очередь, отвечал за достижение главной цели – миграцию информационных систем на территорию РФ.

Для каждого проекта были четко определены свои цели и содержание, свой устав, свой менеджер проекта и своя команда. Если проект предполагалось выполнять собственными силами, а формирование однозначного ТЗ представлялось маловозможным, мы применяли Agile-подходы к управлению таким проектом. В других ситуациях – четкое ТЗ для подрядчика и планирование по Waterfall (Agile – гибкая, Waterfall – каскадная модели разработки проекта. Прим. редактора). Исходя из согласованного подхода к управлению, выбирали менеджера на данный конкретный про-

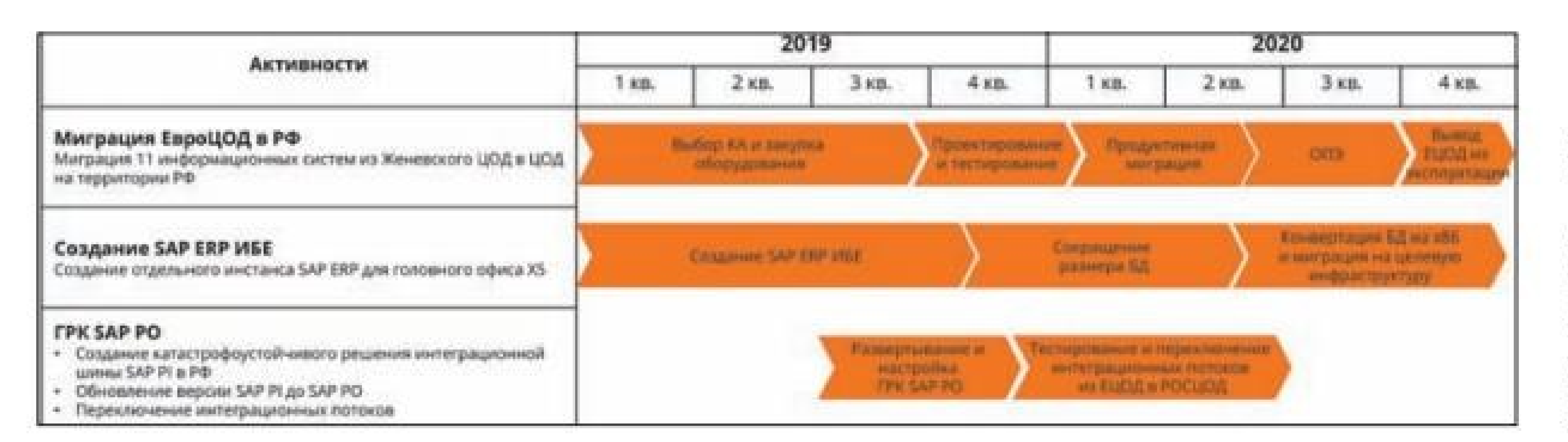


Рис. 2. Сроки реализации программы "Миграция ЕЦОЦ"

ект, поскольку талант планировать и страсть работать по Agile редко встречаются в одном человеке.

Устав программы проектов

На уровне устава программы проекты объединялись по тому же принципу, как рамочный договор объединяет несколько заказов общими условиями. Часть ключевых менеджеров и технических экспертов формировали команду программы и обеспечивали слаженность технических и управленческих решений для проектов, входящих в программу.

Команда программы могла оперативно перераспределить ресурсы от одного проекта другому. Менеджер головного проекта одновременно являлся руководителем программы.

Устав программы проектов ("рамочный договор") требовал жесткой фиксации скоупа, бюджета и сроков в уставе отдельного взятого проекта, причем скоуп, сроки и бюджет самой программы могли быть оперативно скорректированы решением управляющего комитета программы. Принцип корректируемого скоупа позволил оперативно разработать и согласовать устав программы, не описывая мельчайшие детали проектов, время инициации которых еще не пришло.

Сроки реализации

В проектах программы одновременно работало от 120 до 200 (в зависимости от периода) специалистов компании и подрядных организаций. Общий срок жизни программы от ее инициации и до завершения последнего из проектов составил 18 месяцев (рис. 2), при том что миграция информационных систем была осуществлена всего за три месяца. Остальное время ушло на подготовку к переезду, опытную эксплуатацию КТС в РФ, высвобождение площадей ЕЦОД и подведение итогов программы.

7 ключевых эффектов от выбранного подхода

Реализованный нами подход позволил:

1. Синхронизировать проекты программы по целям, скоупу и срокам, примененным техническим решениям.
2. Распределить ответственность и нагрузку на менеджеров проектов.
3. Сократить суммарные издержки на реализацию проектов.
4. Исключить инциденты прерывания ИТ-сервисов, обусловленные миграцией систем.
5. Реализовать гибкие методологии в одних проектах и старый добрый "вотерфолл" в других.
6. Обеспечить синхронизацию проектов программы и задач из операционной деятельности ИТ.
7. Создать лучшую управляемость со стороны заказчиков и владельцев, объединенных в один управляющий комитет программы проектов.

Итогом реализации программы стало сокращение расходов на инфраструктуру SAP-систем, предсказуемый рублевый бюджет на услуги Collocation и катастрофоустойчивое решение для интеграционной шины, связывающей несколько сотен информационных систем, эксплуатируемых в X5.

Надеюсь, управление программами проектов и далее будет практиковаться для достижения масштабных целей в X5, а также поможет вам в решении управленческих задач. Попробуйте "микросервисную архитектуру" в проектном управлении! ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА ЭКСПЕРТА

Видеоаналитика для ритейла: цифры важнее, чем картинка



Андрей Христофоров
Коммерческий директор ITV Group

Собственникам торговых сетей и гостинично-ресторанного бизнеса становится все менее интересно просматривать архивы видеозаписей со своих объектов – видео уходит на второй план и становится инструментом для перепроверки инцидентов. В приоритете у заказчиков видеоаналитика и получаемые с ее помощью цифры, которые дают объективную информацию для оценки и оптимизации бизнес-процессов. Поэтому большое значение приобретает удобство интерфейса системы отчетов и возможность ее настройки под требования конкретного бизнеса.

До недавнего времени аналитика для большинства заказчиков оставалась просто набором инструментов, входящим в стандартное ПО для видеонаблюдения. Сегодня пришло понимание, что эти технологии могут косвенно влиять на выручку и, прежде всего, позволяют бизнесу стать контролируемым. Подсчет посетителей, в том числе уникальных, модули определения "горячих/холодных" зон, анализ очередей на кассе, контроль кассовых операций и выкладки товара – технологии, помогающие оптимизировать бизнес-процессы.

Первое место по популярности удерживает модуль распознавания лиц. Причем его стараются применять как для безопасности – сравнение с черными списками посетителей, так и для продаж и маркетинга – применение систем скоринга и лояльности. Все чаще лица детектируют как при входе в магазин, так и в кассовой зоне – решение, которое помогает выделить тех, кто уходит без покупок, проанализировать видеозаписи их пребывания в магазине и понять причину этого.

В дорогих ресторанах и отелях для повышения качества сервиса востребованы сочетания модулей распознавания лиц и автомобильных номеров, позволяющие персоналу подготовиться к встрече VIP-клиента, а также снижающие вероятность угона машин с парковки заведения.

Существуют технологии, подсчитывающие, сколько людей проходит мимо торговой точки за день и сколько из них заходит. Если такая аналитика и имеет какую-то степень погрешности, то на больших числах статистика выравнивается, вырисовывается общий тренд, и предприниматель понимает, работает ли запущенная им реклама заведения или стоит что-то менять.

Наблюдается большой спрос на синергию видеоаналитики и системы лояльности: первая "узнает" клиента, а вторая показывает, что он обычно покупает. За счет этого, во-первых, удается вызвать "вау-эффект": у клиента возникает ощущение, что его запомнили и выделили из всех остальных посетителей. Во-вторых, продавец может сделать клиенту персональное предложение с учетом его индивидуальных потребностей. Все это помогает бизнесу допродавать товары и услуги.

Повышается интерес ритейла и к сложной нейросетевой аналитике, при этом заказчики нередко переоценивают возможности современных технологий. Приведу пример: владельцы бизнеса хотят иметь инструменты для анализа быстроты реакции продавца на вошедшего в магазин покупателя. Теоретически такой сценарий реализовать возможно, но на текущий момент все упирается в большие погрешности. Однако технологии совершенствуются именно под влиянием спроса на них, и, вероятно, скоро мы увидим системы, которые надежно решают подобные сложные задачи. ■

Современные технические решения по комплексной блокировке музейных и ювелирных витрин

В статье рассмотрены основные аспекты и проблемы организации противокриминальной защиты музейных и ювелирных витрин. Представлен вариант организации комплексной защиты витрин с использованием новых технических средств обнаружения



Александр Федин
Старший научный сотрудник
ФКУ НИЦ "Охрана" Росгвардии



Евгений Химцов
Научный сотрудник
ФКУ НИЦ "Охрана" Росгвардии



Для хищения ювелирного изделия из витрины магазина нарушителю достаточно протянуть к нему руку

Надежная блокировка витрин может быть достигнута только с применением тактики охраны и средств обнаружения (извещателей), соответствующих особенностям данной задачи

Объекты культурного наследия, такие как музеи, выставки, храмы, являются местами концентрации предметов, имеющих большую ценность, как нематериальную (художественную, историческую, духовную), так и материальную (финансовую). По этой причине утрата или повреждение находящихся в них экспонируемых ценных предметов (далее – экспонатов) вызывают, как правило, широкий общественный резонанс и наносят значительный материальный ущерб, поэтому их предотвращение является важнейшей задачей.

Ювелирные магазины представляют собой места концентрации изделий из драгоценных металлов и камней. При этом круг злоумышленников, которые потенциально могут совершить ограбление таких магазинов, шире, чем для объектов культурного наследия, по причине более легкого нелегального сбыта украденных изделий из-за отсутствия у них культурной ценности и, следовательно, отсутствия государственного учета, уникальности и общественного внимания.

Основными угрозами объектам культурного наследия и ювелирным магазинам являются криминальные посягательства, связанные с похищением экспонатов, значительная часть которых, как правило малогабаритных или особо ценных, демонстрируется в специальных закрытых остекленных конструкциях, таких как витрины, киоты, стеновые ниши (далее – витрины). Следует отметить, что витрины являются практически единственным средством инженерно-технической укрепленности, предохраняющим экспонаты от несанкционированного воздействия или кражи в часы приема посетителей.

Однако очевидно, что витрины не являются неприступной крепостью и сами нуждаются в защите, заключающейся в обнаружении различных видов криминальных воздействий на них.

Тактика охраны витрин

Надежная блокировка витрин может быть достигнута только с применением тактики охраны и средств обнаружения (извещателей), соответствующих особенностям данной задачи.

Тактика охраны витрины должна предполагать организацию как минимум двух рубежей охраны:

- рубежа, предназначенного для обнаружения разрушения остекленных поверхностей витрины и открывания ее дверцы или иных подвижных элементов, в зависимости от конструкции;
- рубежа, предназначенного для обнаружения перемещения во внутреннем пространстве (объеме) витрины.

В определенных случаях может возникнуть необходимость организации дополнительного рубежа, предназначенного для обнаружения изъятия витрины вместе с содержимым (актуально для витрин с небольшими массой и габаритными размерами) либо изъятия из витрины отдельных экспонатов, обладающих особой ценностью.

Основным отличием тактики охраны витрин от тактики охраны помещений является объект обнаружения. Анализ габаритных характеристик большинства витрин показывает, что для изъятия экспоната из витрины нарушителю нет необходимости, а часто и возможности проникать в ее пространство всем телом, достаточно протянуть к нему руку. Следовательно, для блокировки внутреннего пространства витрины требуется применение извещателя, обеспечивающего обнаружение перемещения руки в зоне обнаружения.

Специализированные извещатели

Исходя из сказанного выше, для охраны витрин настоятельно рекомендуется применять специализированные извещатели, предназначенные для решения указанной задачи.

Извещатели первого поколения

В разное время отечественными предприятиями было освоено серийное производство таких изделий, основанных на различных физических

принципах: ультразвукового извещателя "Витрина", пассивного инфракрасного "Икар-ШМР" (на сегодняшний день оба сняты с производства) и активного инфракрасного "СПЭК-7-6". Эти изделия, помимо несомненных достоинств, обладали и рядом недостатков, обусловленных их физическими принципами:

- невозможность блокирования внутреннего объема охраняемой витрины для извещателя "СПЭК-7-6";
- невозможность обнаружения разрушения остекленных поверхностей охраняемой витрины;
- технические сложности создания беспроводного исполнения (кроме извещателя "Икар-ШМР").

Современные извещатели

В 2020 г. в соответствии с подготовленным Минкультуры России и согласованным с Росгвардией Планом основных мероприятий по обеспечению охраны музейных предметов и безопасности в музеях по заданию Главного управления вневедомственной охраны Росгвардии был разработан специализированный совмещенный радиоканальный извещатель, предназначенный для организации комплексной защиты витрин от несанкционированных воздействий и кражи экспонатов (драгоценностей).

Извещатель обладает малогабаритным корпусом, имеет автономное электропитание и совмещает в себе два независимых канала обнаружения:

- пассивный оптико-электронный канал, формирующий объемную зону обнаружения и предназначенный для обнаружения руки человека (обычные пассивные оптико-электронные инфракрасные извещатели надежного решения этой задачи не обеспечивают из-за несоответствия объекта обнаружения);
- пассивный звуковой канал, предназначенный для обнаружения разрушения различных видов стекол, которые могут применяться для остекления витрин.

Сочетание двух каналов обнаружения позволяет обнаруживать два основных вида криминальных воздействий на витрины и осуществлять их эффективную комплексную блокировку. Выбор физического принципа действия одного из каналов, основанного на регистрации температурного контраста между рукой нарушителя и окружающими предметами (фоном), позволяет реализовать следующие преимущества, важные при организации охраны витрин:

- отсутствие необходимости в зоне отчуждения за счет непрозрачности стекла в используемом ИК-диапазоне длин волн, что позволяет обеспечить доступ посетителей непосредственно к витрине, находящейся под охраной;



Утрата ценных экспонатов вызывает широкий общественный резонанс и наносит значительный материальный ущерб

Малогабаритные беспроводные извещатели позволяют обеспечить комплексную блокировку музейных и ювелирных витрин, используя современные технические решения

- вариативность типа зоны обнаружения, позволяющая создавать в будущем исполнения извещателя с различными типами зон для охраны витрин различной конфигурации.

Конструкция извещателя для охраны витрин позволяет закреплять его в углах охраняемой витрины непосредственно на стекло при помощи двусторонней монтажной ленты (скотча). Для контроля крепления извещателя во время эксплуатации он имеет встроенные средства обнаружения отрыва от монтажной поверхности.

Небольшие габаритные размеры извещателя позволяют минимизировать нарушения художественного замысла экспозиции, размещенной в витрине, и не препятствовать осмотру экспозиции посетителями.

Низкое токопотребление за счет отсутствия формирования собственной рабочей среды позволяет использовать извещатель для применения в составе беспроводной охранной системы.

Отсутствие необходимости прокладывания проводных линий электропитания и шлейфов сигнализации (в отличие от рассмотренных выше проводных извещателей) обеспечивает:

- минимизацию повреждений охраняемых витрин, а также интерьеров, в которых они располагаются;
- возможность применения извещателя для охраны витрин "островного" типа, доступ к которым возможен со всех сторон;
- возможность быстрого изменения места установки при изменении композиции как в охраняемой витрине, так и объекта в целом (с изменением места расположения витрины).

Таким образом, малогабаритные беспроводные извещатели позволяют обеспечить комплексную блокировку музейных и ювелирных витрин, используя современные технические решения.

Список литературы:

1. Климов А.В., Рябцев Н.А., Федин А.Н. Перспективы развития средств обнаружения несанкционированного проникновения в помещения и хранилища ценностей // Научный интернет-журнал "Технологии техносферной безопасности". 2016. № 4 (68). С. 1–7.
2. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений (Р 78.36.044–2014) / Климов А.В., Рябцев Н.А., Членов А.Н. и др. М.: ФКУ НИЦ "Охрана" МВД России, 2014. 92 с.
3. ГОСТ Р 50777–2014 Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний [Текст]. Введ. 01.01.2016 взам. ГОСТ Р 50777-95 (МЭК 60839-2-6:1990). М.: Стандартинформ, 2014. ■

Ваше мнение и вопросы по статье направляйте на **ss@groteck.ru**

Редакция советует

В статье рассмотрены основные аспекты и проблемы противокриминальной защиты музейных и ювелирных витрин. Рассказано о тактике охраны витрин, организации их комплексной защиты с использованием новых технических средств обнаружения.

Современные охранные извещатели производят российские компании "АРГУС-СПЕКТР", "Магнито-Контакт", научно-внедренческое предприятие (НВП) "Болид". Подобные извещатели есть также в ассортименте крупнейшего российского дистрибьютора систем безопасности – компании "АРМО-Системы", которая предлагает оборудование ведущих мировых производителей, информирует и обучает заказчиков, обеспечивает высокий уровень сервиса.



Константин Сергеев

Директор по безопасности ТС "Монетка", преподаватель курса "Корпоративная безопасность" УрГЭУ, руководитель объединения "Союз руководителей служб безопасности бизнеса", член Общественного совета МВД России по г. Екатеринбургу

Цифровое будущее ритейла

Управление рисками товарных потерь торговой сети, оснащенной кассами самообслуживания

Касса самообслуживания, Self Checkout (SCO), – электронно-механическое устройство, работающее без кассира (оператора), позволяющее реализовать процесс самообслуживания оплаты товара в магазинах розничной торговли. SCO, являясь альтернативой традиционным кассам розничных сетей, обеспечивают существенные конкурентные преимущества за счет создания условий для быстрой покупки и минимизации операционных затрат магазина



Касса самообслуживания Self Checkout (SCO)

Историческое отступление

С 1958 г. в городах СССР перешли с кондукторной на кассовую систему оплаты проезда. Пассажир сам оплачивал проезд, бросив монету в кассу и открутив билет. Позже появились компостеры – предоплатная система. В годы развитого социализма считалось, что совесть – лучший контролер. Высокая социальная ответственность заставляла практически каждого гражданина следить за оплатой своего проезда. Контролеры при этом также были включены в систему профилактики неоплат.

В сфере торговли товарами массового спроса, в том числе пищевыми продуктами, такого доверия клиентам не оказывалось. До появления универсамов покупателям в магазинах требовалось совершить следующую последовательность действий: пройти в отдел, выбрать все необходимые товары, получить от продавца общую сумму покупки, отправиться на кассу, заплатить, получить чек и с ним вернуться к прилавку, чтобы забрать свой товар.

С распадом СССР и последующим катастрофическим падением сборов за проезд транспортные предприятия снова перешли на кондукторную систему оплаты проезда. В большинстве городов России до сих пор сбор оплаты проезда обеспечивают кассиры.

Наше время

По оценке лаборатории "СберИндекс" и ИТ-компании "Платформа ОФД", доля безналичного торгового оборота в России увеличивается каждый год и в IV квартале 2020 г. составила 55,9%[1]. Такая тенденция является потенциалом для постепенного отказа от наличных платежей и перехода к SCO, оснащенным только эквайринговой оплатой. Это позволяет большинству российских продуктовых торговых сетей с небольшим запозданием поддержать мировой тренд автоматизации магазинов на базе технологий Self Checkout.

На данный момент идет переход к параллельному функционированию "традиционных" касс и касс самообслуживания. Некоторые магазины устанавливают кассы самообслуживания для разделения потока покупателей с небольшим числом товаров в корзине и покупателей с тележками. Пандемия COVID-19 также придала импульс развитию SCO, для снижения контакта покупателей с персоналом магазина.

Виды SCO

На кассе магазина товар должен быть подсчитан, зафиксирован в чеке и оплачен. От четкой и слаженной работы касс зависит прибыль магазина.

Категории магазинов, использующих технологию касс самообслуживания обширны, среди них:

- FMCG (Fast Moving Consumer Goods) – товары повседневного спроса, в том числе продукты питания;
- DYI (Do it Yourself) – рынок строительно-отделочных материалов.

В процессе тестирования категории Non-food – промышленные непродовольственные товары. К ним относятся электрическое и электронное оборудование, бытовая техника и радиоаппаратура, игрушки, товары для интерьера, спортивные товары, канцелярские принадлежности, обувь и текстиль, косметические средства и товары бытовой химии.

Из разнообразия технических и ИТ-программных решений в зависимости от концепции кассы самообслуживания можно выделить:

- Fixed Scan and Go – фиксированные (стационарные) SCO;
- Scan and Go – покупатель получает автономный сканер на входе;
- Mobile Scan and Go – покупатель использует свое личное мобильное устройство как сканер.

Наиболее развитое в России направление – фиксированные SCO, в свою очередь, также подразделяются на несколько технических и программных решений. Есть SCO с дополнительными контрольными технологиями по общему весу товаров, а также SCO, включенные в закрытую зону (остров) с автоматическим контролем выхода. У большинства касс самообслуживания есть свой светозвуковой маяк, подающий сигнал персоналу при необходимости уделить внимание кассе. Как правило, в зоне самообслуживания находится сотрудник, который следит за происходящим на 4–6 кассах и помогает покупателям совершить покупку.

[1] *СберИндекс. Рейтинг "безналичных" городов и регионов России. Итоги IV кв. и 2020 г. [Электронный ресурс]. – URL: https://sberindex.ru/ru/researches/reiting-beznalichnykh-gorodov-i-regionov-rossii-itogi-iv-kv-i-2020-g*

Плюсы создания доверительной среды при реализации товаров

Возможность доверить покупателям самостоятельно сканировать и оплачивать покупки несет в себе конкурентные преимущества:

- кассы самообслуживания помогают бизнесу работать без простоев и перерывов, способствуют сокращению расходов на персонал и минимизируют кассовые махинации с его участием;
- дают возможность экономить на аренде дорогостоящих торговых площадей (на месте одной обычной кассы умещается две, а то и больше SCO);
- способствуют росту продаж благодаря уменьшению очередей и созданию условий для быстрой покупки.

Минусы ввода технологий Self Checkout

Товарные потери – обратная сторона получаемых при внедрении технологии Self Checkout преимуществ.

Заслуживающим внимания является международное исследование 2018 г. "Касса самообслуживания в розничной торговле: оценка влияния на убытки". Анализ данных 13 торговых сетей и 140 млн транзакций на SCO показал, что, если в магазине 50% транзакций обрабатывается через SCO, можно ожидать, что его потери будут на 75% выше, чем средний показатель, установленный для розничной торговли продуктами питания[2]. К примеру, если норматив неизвестных (ревизионных) товарных потерь продуктового магазина составлял 0,45%, то с вводом системы SCO стоит ожидать увеличения уровня потерь до 0,79%.

Увеличение количества товаров в чеке равняется увеличению вероятности возникновения ошибки. Когда у покупателя более 50 товаров в корзине, вероятность того, что он совершит хотя бы одну ошибку при сканировании, составляет 60%.

Выделяют 5 типовых точек потерь на SCO:

1. Несканирование части товара. Манипуляции с уменьшением количества товара, попадающего в чек. Согласно исследованию, 77% потерь на SCO связаны с этим видом манипуляций.

2. Вынос товара без оплаты (имитация оплаты товара).

3. Манипуляции с уменьшением веса товара, попадающего в чек.

4. Подмес. Смешивание дорогого весового товара с похожим дешевым и оплата как дешевого.

5. Неправильное сканирование или подмена продукта, когда покупатель сканирует штрихкод дешевого продукта, а кладет дорогой.

Управление рисками товарных потерь

К "традиционным" способам совершения магазинных краж (шоплифтинга) теперь добавились и махинации на кассах самообслуживания.

На интернет-ресурсе "Судебные и нормативные акты Российской Федерации" (www.sudact.ru) по запросу "касса самообслуживания" на дату написания публикации представлено 8 497 документов, и не все из них связаны именно с хищением товаров с SCO. Практика административного и уголовного наказания по данным видам правонарушений и преступлений в России только формируется и имеет сложности с доказательной базой умысла хищения через манипуляции на SCO, а не случайными ошибками.

Ключом для управления рисками товарных потерь является комплексный подход, основанный на создании выделенной контролируемой доверительной среды и формировании сдерживающих от хищений факторов.

От расположения самих модулей SCO, системы освещения, видеонаблюдения, включения персонала в систему профилактики краж, контрольных процедур зависит многое, в том числе и формирование у покупателей социально одобряемой модели поведения.

Отдельным блоком стоит отметить аналитическую работу и проактивный мониторинг действий покупателей на кассе, совмещенный с видеоаналитикой. Наиболее интересен в профилактике краж на SCO переход от системы распознавания лиц к системе контроля поведенческих признаков и персонализированной профилактике краж, анонсированной в 2021 г. компанией "BIT", разработчиком ИАС "СТОП Шоплифтер" совместно с компанией "НТехЛаб". Накопленный опыт коллаборации крупнейших торговых сетей по профилактики магазинных краж позволяет реализовывать амбициозные проекты по SCO с минимизацией доли неизвестных потерь, осуществлять переход от устаревшей и затратной системы антикражных решений к персонализированному контролю и предупреждению краж.

Большой технологический шаг сделан и в видеоконтроле на базе машинного зрения и искусственного интеллекта – сверка соответствия товара в чеке и на весах. На SCO, оснащенных весами с распознаванием продуктов, подменить один товар другим практически невозможно. Выбирать товар на таких SCO не нужно, все делается автоматически, система умеет также распознавать сорта фруктов и овощей, которые в дальнейшем попадают в чек.

Телеметрия работы SCO также позволяет включать различные сценарии и протоколы контрольных мероприятий по фродовым транзакциям и проводить оперативное оповещение о событиях по заданным параметрам. Настроенные автоматические алгоритмы, состоящие из нескольких параметров, позволяют выделять "тревожные транзакции" и рецидивные кражи, помогают в создании доказательной базы, направленной на быстрое и полное раскрытие преступлений. Так может быть поставлена на контроль оплата ранее скомпрометированной на хищениях банковской карты, нехарактерные повторяющиеся виды и веса товаров, временные промежутки сканирования, отказы от покупки и т.д.

Магазинные кражи – одно из самых распространенных правонарушений в России, которое носит в первую очередь социальный характер. Создание даже высокотехнологичных барьеров и контрольных мероприятий самими ритейлерами минимизирует кражи, но не решает проблему в целом. Уход государства в сторону декриминализации проблемы, массовые отказные материалы полиции по фактам мелких хищений – путь замалчивания, но не решения проблемы.

Безусловно, данный вопрос должен решаться посредством государственного партнерства с торговыми сетями и общественными организациями, с использованием передовых технологий и видеоинфраструктуры для создания единого контура безопасности, на примере системы "Безопасный город". Немаловажно также внедрение специализированых социальных программ с акцентом на профилактику подростковой преступности и формированием в обществе нетерпимости к правонарушениям, в том числе к магазинным кражам.

Анализ данных 13 торговых сетей и 140 млн транзакций на SCO показал, что, если в магазине 50% транзакций обрабатывается через SCO, можно ожидать, что его потери будут на 75% выше, чем средний показатель, установленный для розничной торговли продуктами питания

Заключение

Ритейл является одной из самых динамичных отраслей экономики. Оплаты по технологии Face ID, персонализированные предложения с прогнозом потребностей в покупке и поддержка системы лояльности покупателей, умные полки, определенные алгоритмы формирования заявок на поставки необходимых товаров в определенную торговую точку – эти и многие другие инновации уже тестируются в ритейле.

Внедрение таких технологий, как кассы самообслуживания, – всего лишь этап перехода офлайн-розницы к "магазину будущего" Take&Go.

Безусловно, развитие эффективных мер предотвращения потерь движется в направлении ИТ-контроля, основанного на нейросетях, автоматического обогащения информации и проактивного персонализированного контроля. Уже сейчас поиск баланса между "быстро" и "точно и под контролем" становится настоящим вызовом для специалистов по безопасности в ритейле, формируя новый подход к управлению рисками. ■

Ваше мнение и вопросы по статье направляйте на



[2] *Adrian Beck. Self-Checkout in Retail: Measuring the Impact on Loss [Electronic resource]. – URL: https://www.ecrloss.com/research/self-checkout-research*



Андрей Чикун
Руководитель ИТ-департамента компании "Лозанж" – официального дилера Renault в Беларуси

Нейросетевая видеоаналитика в автосалонах

Опыт дилера в Беларуси

Дилерская сеть "Лозанж" насчитывает множество дилерских центров, территориально разнесенных по всей Беларуси, это просторные шоурумы с современными сервис-зонами, обширными складами запчастей и удобными парковками. Прогрессивный стиль работы компании учитывает применение самых передовых технологий не только для максимального комфорта на всех стадиях обслуживания, но и для высокого уровня безопасности объектов. Андрей Чикун, руководитель ИТ-департамента, рассказал, какие системы помогают компании эффективно решать задачи безопасности, экономить ресурсы и увеличивать показатели даже в условиях пандемии



– Автосалон – объект с высоким риск-фактором. Какие важные моменты необходимо учитывать при организации охраны салона? Какие наиболее актуальные охранные мероприятия выполняются, в том числе в рамках антитеррористической защищенности?

– Беларусь – относительно спокойная страна, и внешних рисков на самом деле не так уж и много. У нас есть собственные парковки для хранения автомобилей. На местах присутствуют сотрудники внутренней охраны, которые смотрят, чтобы машины корректно выезжали и посторонние не проникали на территорию. Раньше мы очень переживали, что кто-то кинет бутылку через забор или захочет попасть на парковку и что-то украсть, но за 12–13 лет моей работы такого не было ни разу. Максимум люди в состоянии алкогольного опьянения могли зайти, да и то на открытую территорию автоцентров, где нет заборов. Поэтому повторюсь: внешние риски крайне невелики. Структура управления и мониторинга централизованная: все задачи, от администрирования до разработки и безопасности, находятся в едином центре, а не в автосалонах.

Что касается антитеррористических мероприятий, то реальных терактов в стране не было. Для относительно мирной Беларуси эта задача не столь актуальна.

Самая большая проблема в нашем бизнесе – внутренние риски. Я не беру в расчет кражи канцтоваров и туалетной бумаги, но, если люди выносят запасные части, это беда.

На заре работы компании были случаи, когда сотрудники создавали фиктивных оптовых покупателей запасных частей и продавали им розничный поток.

Пример: приходили клиенты-оптовики и, на первый взгляд, все шло хорошо. А на самом деле человек, отвечающий за продажу запчастей, по документам создал несуществующего оптовика с вымышленными ФИО, у которого была максимальная скидка 15–20%. Часть покупок входящего потока людей (5–10 заказов в день) оформлялись на имя этого самого оптовика, а значит, компания должна была сделать скидку до 20%, которую клал себе в карман ответственный сотрудник. С людей брал реальные деньги, оформлял на оптовиков, а разницу забирал себе. Сейчас все такие схемы у нас быстро раскрываются и проверяются.

Самая большая проблема в нашем бизнесе – внутренние риски. Я не беру в расчет кражи канцтоваров и туалетной бумаги, но, если люди выносят запасные части, это беда

В таких случаях необходимо разделять оптовые и розничные каналы продажи запасных частей. Есть отдел, который занимается только оптовыми продажами и никак не пересекается с розницей.

И наконец, еще один очень актуальный вопрос – утилизация запасных частей, которые меняются по гарантии или в ходе кузовного ремонта. Например, на кузовной участок приезжает автомобиль на ремонт, который оплачивает страховая компания. Клиент по закону вправе забрать запчасти, которые были заменены. Допустим, в машине поврежден бампер, немного сдвинута фара, а при демонтаже оказывается, что поломано крепление фары. Она сама рабочая, но, согласно технологиям ремонта, ее необходимо менять. Не допускаются ни пайка, ни сварка. Клиенту по большому счету все равно, что с этой запчастью будет дальше. Мы даже специально вводили форму, в которой он должен поставить галочки, если старые запчасти ему нужны, и расписаться. Очень небольшой процент людей действительно расписывались. Клиент даже не знал, что нужно было приехать и забрать запчасть. Фара меняется, страховая платит, клиент забирает готовую машину, а запчасти, которые менялись по кузовному ремонту или по гарантии, попадают на вторичный рынок.

Я сам страхую автомобиль на полное каско и без износа. Да, это стоит 2–4% от стоимости автомобиля, но это избавляет от любых проблем. Поцарапали, ударили, попал в ДТП и сам виноват… Все покрывает страховая (главное, чтобы трезвый был).

Из своего личного опыта: я когда-то сам покупал б/у кузовные запчасти. И в 2015 г. со мной произошел неприятный случай. Ехали с коллегой по трассе и на скорости чуть больше 120 км/ч вылетела левая фара (вырвало проводку, поцарапало крыло, фара вдребезги), хорошо, что никому не прилетело из попутно идущего транспорта. Виной всему оказались сломанные и склеенные крепления фары.

С одной стороны, возникает вопрос: какая разница, ведь запчасти оплачены и клиенту они не нужны. Почему их нельзя просто выкинуть или отдать кому-то, а надо правильно утилизировать? Потому что для компании это прямые убытки: на вторичном рынке куча б/у запчастей, и компания не

может продавать новые. От этого страдают все, в том числе и клиенты, и страховая компания. Люди не страхуют автомобили, потому что на рынке все запчасти всегда в доступе. И наоборот, когда они понимают, что б/у запчастей немного, то лучше застраховать машину по каско – это выгоднее и производителю запасных частей, и поставщику, и страховой компании. С такими сценариями мы продолжаем бороться.

Сейчас все точки, где внедрена нейросетевая видеоаналитика, очень эффективны. Снижается количество нарушений, повторный заезд на территорию происходит только с открытием повторных документов и т.д. Руководство отмечает, что система дает свои плоды

– А как правильно должна строиться работа в описанном примере с заменой запчастей?

– Если машина приехала на кузовной ремонт с поврежденным креплением фары, то сотрудник должен взять эту фару, пойти на склад, показать документы о том, что фара меняется, сдать старую и получить новую. Дальше старые запчасти откладываются в отстойник, перевозятся в пункты назначения и утилизируются под видеонаблюдением. Специальная комиссия подтверждает, что была произведена утилизация. Если же клиент сообщает, что ему нужна старая запчасть, то ее выдача происходит через внутренние службы безопасности, которые проверяют, действительно ли это тот самый клиент.

Еще одна очень частая проблема, особенно на удаленных площадках, – это несанкционированные ремонты, не соответствующие открытым заказ-нарядам. Например, машина заезжает в цех, на въезде мастер-приемщик показывает охране документы, по которым нужно произвести снятие колеса, а на деле перебирается половина подвески. В столице это контролируют, но если взять небольшие города, где каждый друг другу кум, сват и брат, то это реальная проблема. В таких ситуациях нам помогают технологии, в частности система нейросетевой видеоаналитики.

– Какие задачи решает такая система в автосалоне?

– В нашем случае она:

1. Следит за мастерами-приемщиками и нарушениями регламента. Если компания дает рекламу и телефоны разрываются, но в столе заказов нет ни одного человека больше минуты–двух (везде свои регламенты) – это нарушение.

2. Сверяет с внутренней системой въезд на территорию без документов. Если машина заехала, но никаких документов по ней не открыто, это сигнал для дальнейшего "разбора полетов". Дальше машина заезжает в цех на подъемник, и система присваивает ей номер и место, а также анализирует загрузку подъемников и цеха. Часто сотрудники заявляют, что сами будут смотреть загрузку по учетной системе, но такой подход не совсем точный. Одно дело, когда вам необходимы синтетические цифры, другое – реальные. Например, по всем нормативным актам установка колеса занимает 10 минут, замена мотора – восемь часов. А по факту на снятие/установку колеса уходят три минуты, на замену мотора – семь часов, то есть данные учетной системы расходятся с реальными цифрами.

Везде работают люди, кто-то более опытный и выполняет работу быстрее. Никто не говорит про нарушение технологий ремонта, нет. Все делается строго по технологиям и обязательно проверяется мастером цеха.

Так у руководства появилась необходимость в понимании реальной загрузки цеха и наличии подъемников, что и показывает система.

Поэтому случаи, когда открыли заказ-наряд на снятие/установку колеса, а машина провисела четыре часа, сразу исключаются.

3. Отслеживает мойки. Например, на заехавшую машину открыта технологическая мойка на 15 минут, а на посту она находится 40 минут. Система сразу показывает отклонения. Аналитик смотрит по видео, что происходит. Одно дело – просто помыть машину снаружи, а другое дело – комплексная мойка, когда вся машина разбирается, снимаются коврики и т.д.

Сейчас все точки, где внедрена нейросетевая видеоаналитика, очень эффективны. Снижается количество нарушений, повторный заезд на территорию происходит только с открытием повторных документов и т.д. Руководство отмечает, что система дает свои плоды.

– То есть на ваших объектах технологии видеоаналитики уже во многом заменили человека?

– Вот что важно понимать: нейросетевая видеоаналитика не основное наше оружие. Основное оружие – это мозги, а главная задача команды – включать мозги и анализировать все, что происходит. Зачастую это игра в кошки-мышки, когда от нас бегают и пытаются сделать себе жизнь лучше, а мы бегаем и стараемся найти, где сотрудники, "улучшая" жизнь, наносят урон клиентам и компании. Например, аналитика очень хорошо справляется с аспектами неправомерного въезда на территорию, более длительными ремонтами и мойкой, разделением по цехам (кузовной и не кузовной). Это очень классный инструмент, который показывает, где возможны проблемы и где необходимо принятие мер. Но система не решит проблему за вас.

Технологии должны помогать развивать бизнес, а не тормозить его. Например, по этой причине мы убрали Face ID. Раньше мы считали входящий трафик, распознавали людей, но администраторам было очень трудно сверять лица с базой, создавать события. Они все чаще делали это в конце дня, перед закрытием автосалона, вспоминая, сколько примерно было клиентов и проставляя данные наугад. Фактически мы получали очень много мусора. В результате мы отказались от этой идеи, так как у нее оказалось больше минусов, чем плюсов. У бизнеса просто не было потребности в таком распознавании.

Есть еще несколько причин, почему я говорю, что самое важное – это мозги и качественные кадры, которые могут за всем следить:

1. Когда машин продается и ремонтируется много и поток клиентов хороший, руководство меньше обращает внимание на определенные вещи. Но с началом пандемии начался спад, и стало понятно, что необходимо оптимизировать затраты. На менеджеров нагрузка снижается, но на ИТ-отдел возрастает, так как нужно проанализировать, почему происходят те или иные вещи, заменить функции людей технологиями и т.д.

2. По условиям нашей бонусной программы клиенту выдается карточка, на которую начисляются баллы. В дальнейшем их можно потратить в дилерской сети на услуги или товары. И начинаются манипуляции и махинации со







Честность – это очень важное качество в сотрудниках для руководства компании. Если где-то оплошал, то приди и честно скажи об этом. Не надо, как нашкодивший котенок, закапывать и прятаться в углу с мыслью "а вдруг не заметят"

стороны тех же мастеров-приемщиков и продавцов. Мы сделали максимально лояльную программу для клиента, когда он может взять карточку у родственника или жены/мужа и рассчитаться ей. Например, если машину на сервис загоняет муж, а машина и карточка оформлены на жену, мы не можем запретить клиенту расплатиться ей. Поэтому карты абсолютно обезличены, на них не написаны ни имя, ни фамилия, ни номер. Это просто карта, которую надо приложить к считывателю, и только тогда произойдет списание. Если клиент вдруг забыл карту, мы допускаем начисление баллов, но списать их можно только при физическом наличии карты. Далее стали происходить удивительные вещи. Сотрудники, которые анализируют списания и смотрят отчеты, заметили аномалии. К примеру, клиент привозит на ремонт автомобиль и хочет расплатиться баллами, но выясняется, что он накопил баллы, производя в течение месяца ремонт 20 разных автомобилей. Схема предельно понятна: сотрудник сделал карточку на себя или подставное лицо и начал использовать ее по всем заказ-нарядам, накапливая баллы то здесь, то там. В лучшем случае он списывает баллы на ремонт, в худшем – начинает покупать товары (резину, домкраты и т.д.). Такие моменты надо отслеживать, чем мы активно занимаемся.

Кроме того, мы контролируем, чтобы мастер не менял информацию по клиентам, например номер телефона или фамилию. Это связано с тем, что может что-то пойти не так в общении с клиентом (может, конфликт был или он недоволен качеством ремонта). Тогда сотрудник меняет номер телефона на другой, чтобы до клиента нельзя было дозвониться и узнать, как прошло обслуживание. А потом нам ссылается на то, что номер записан со слов самого клиента.

Для нас очень важно, как обслужили клиента, остался он доволен или нет. И если нет, то почему.

Или другой пример – смена фамилии в системе, чтобы списать баллы на якобы жену клиента, который успел накопить много баллов. Все эти схемы надо находить.

Раньше подобных случаев было много. Сейчас сотрудники понимают, что они под пристальным контролем и лучше работать и зарабатывать деньги честно.

Честность – это очень важное качество в сотрудниках для руководства компании. Если где-то оплошал, то приди и честно скажи об этом. Не надо, как нашкодивший котенок, закапывать и прятаться в углу с мыслью "а вдруг не заметят". Если слесарь что-то сделал не так при ремонте (сломал запчасть, ...) и пришел, честно сказал, то к нему никогда не будут применять штрафные санкции. Все мы люди, и все мы можем ошибаться. Руководство всегда идет навстречу, и сотрудник оплачивает новую запчасть по себестоимости. Клиент также всегда получает новую запчасть.

Если слесарь решит все-таки схалтурить, восстановить поломанную запчасть и установить клиенту, то в случае выявления будет очень плохо: слесарь – штраф, мастер цеха – штраф, машина на сервис для полноценного ремонта с новыми запчастями (которые оплатит слесарь уже по розничной стоимости), перед клиентом извинения и, возможно, скидка на следующее ТО (но это уже решает клиентская служба).

– А со стороны посетителей бывают какие-то мошеннические случаи? Или именно со стороны персонала их наибольшее количество?

– Наши сотрудники в основном работают честно, и доля тех, кто хочет "играть не по правилам", очень мала.

– Все помещения и зоны в автосалонах оснащены системами видеонаблюдения и видеоаналитики?

– Не все. В первую очередь необходима минимум одна камера в столе заказов, которая будет смотреть за мастерами – их присутствием или отсутствием. Нужны также камеры на въездных воротах для распознавания госномера и желательно одна-две камеры Fisheye, которые видят, сколько машина пробыла на подъемнике. Причем это не специализированные, а обычные камеры, которые у нас и до этого висели в целях безопасности. На данный момент мы передали видеопоток с этих камер поставщику для обработки и ничего не закупали отдельно. Поэтому при внедрении таких систем важно отталкиваться от своих потребностей и функциональных возможностей, а уже поставщик подскажет, что необходимо для реализации.

– Помогает ли система видеоаналитики улучшать маркетинговые показатели в вашей сфере?

– В современном мире очень многие вещи уходят именно в ИТ-сектор. На сегодняшний день отдел маркетинга – это в первую очередь отдел аналитики, который отслеживает поведенческие факторы и т.д. Вы когда-нибудь задумывались, как влияет, например, цвет автомобиля или сочетание цифр в номере телефона на средний чек? А это все влияет. Многие вещи мы сами разрабатывали и тестировали, другие заимствовали из ритейла. Согласитесь, ведь классно, когда гипермаркет по бонусной карте знает ваши имя и фамилию, когда у вас зарплата, каких производителей вы выбираете, ваши вкусовые предпочтения и что, допустим, по четвергам вы выносите товара на 40 кг, а во вторник и среду – пакетики по 200 г. Он знает, что завтра у вас зарплата, а вы любите рыбу и безалкогольное пиво, поэтому вам можно предложить определенную акцию и сделать СМС-рассылку. А вы думаете: "Спасибо, что напомнили!" При этом можно сразу дать быструю ссылку для оформления заказа, и вам нужно будет только забрать свой товар из магазина.

Так вы экономите самое ценное, что у вас есть, – время. Поэтому маркетинг – это в первую очередь анализ данных, а безопасность – это сохранность данных.

Существует очень много ограничений, которые необходимо отслеживать и внедрять внутри системы, чтобы сторонние люди не получили доступ к данным клиента. Он же явно будет неприятно удивлен, если мастер-приемщик будет знать его имя, фамилию, отчество, адрес и номер паспорта. Максимум, что ему надо знать, – номер телефона и как к клиенту обратиться. А также очень важна корректность созданных событий.

– На ваших объектах работают охранники и операторы, следящие за камерами?

– С точки зрения физической безопасности на каждом объекте действует штат охраны. У нас до недавнего времени охрана была под патронажем государства. Сторож на объекте мог максимум громко кричать или звонить на пост охраны МВД, но не имел права задержать человека. Сотрудники МВД были обязаны в течение определенного времени приехать на вызов. Соответственно, встал вопрос: насколько необходима физическая охрана?

Мы начали оптимизировать штат охраны и уходить в сторону технологий, например интеллектуальной видеоаналитики, чтобы уже система определяла, что зашел человек или подъехала машина, распознала номер

и открыла ворота. Параллельно мы усилили видеонаблюдение и внедрили интеллектуальную видеоаналитику, а картинку вывели на монитор ответственного сотрудника. Если в кадре появляется нарушитель, то он принимает решение – вызвать наряд или пойти проверить, что происходит.
От охраны в классическом понимании мы стараемся сейчас отходить еще и потому, что она обходится дорого.
Пример.
Видеорегистратор стоит 400–500 долларов, цена с жесткими дисками – 800–1500 долларов в зависимости от объема. Даже зарплата обычного сторожа на автостоянке – 200–300 долларов на руки, плюс налоги, и это уже 400–600 долларов. То есть регистратор – это зарплата охранника за два-три месяца. А если вы берете не просто сторожа, а более квалифицированного специалиста, то и еще быстрее окупается. Дальше охраннику надо платить отпускные, больничный, предоставлять форму и т.д.
Кроме того, даже тем охранникам, которые остались, необходимо делать обход. А как контролировать обход? Здесь можно использовать не нейросетевую видеоаналитику, а специальную систему на основе меток типа RFID, которые клеятся по территории. Они стоят три копейки, и ими можно завесить весь автоцентр и всю территорию. У охранника есть прибор, совмещенный с фонариком, который он прикладывает к каждой метке. Затем он возвращается обратно на базу, синхронизирует устройство с системой, а вы видите по контрольным точкам, был ли обход. Другой момент, который необходимо анализировать, – скорость охранника. Для этого замеряется скорость при нормальном спокойном шаге, когда есть возможность посмотреть налево-направо, убедиться, что никого нет. Например, если между точкой А и Б для этого нужно 20 секунд, а система показывает, что у охранника ушло 10 секунд, то, скорее всего, он бежал, причем очень быстро.



От охраны в классическом понимании мы стараемся сейчас отходить еще и потому, что она обходится дорого

– Когда вы задумались о нейросетевой аналитике, как вы выбирали поставщика?
– Это был интересный опыт. На тот момент я очень скептически смотрел на подобного рода системы: на Западе такие решения стоят "космических" денег. Поэтому, когда нам предложили "за рубль канарейку, чтобы басом пела", я считал, что такого не будет. А она действительно начала петь. Нам показали первые результаты, и, честно говоря, я был удивлен.
Затем мы начали клонировать систему и убирать то, что не нужно бизнесу. На старте у нас был анализ и шоурумов, и количества людей, заинтересованных в определенных моделях, и т.д. Но вскоре со стороны бизнеса мы отмели лишнее и оставили только тот оптимальный набор функций, который нам необходим. Важный момент: мы начали оплачивать систему только после того, как она была запущена. При этом сейчас полно поставщиков, которые декларируют одно, но на деле оказывается совершенно другое, да еще и не работает.

– Получается, что производители предлагают очень ограниченный набор функций. И практически никто не может предоставить полноценный охват всех задач предприятия?
– К сожалению, да. Хорошо, если производители предлагают хоть что-то, ведь иногда кажется, что они работают по принципу Кремниевой долины Fake It Till You Make It, то есть "рассказывай клиенту, что все работает, а сам, быстро обгоняя свой визг, это делай". Рынку надо, но продукт не готов.
Я понимаю, как работает ИТ-мир, у нас тоже есть свои разработки и продукты, которые выходят в свет с готовностью чуть выше 30%. На костылях, но работает. (Оговорюсь: для клиента все работает с готовностью, близкой к 100%. Там может быть неоптимальный код по производительности под нагрузкой, там может не быть админпанели для сотрудников.) Выпускаем в свет и смотрим, надо ли это рынку. Не надо – в мусорку. Если что-то нужно изменить в продукте, ИТ-отдел это делает, продукт снова запускается, мы наблюдаем неделю-месяц, если видим, что продукт все равно мертвый, им не пользуются, – однозначно в мусорку. Зачем строить замки и тратить кучу денег и времени? Самое ценное – время!

– Какие системы безопасности необходимо устанавливать в автосалоне? Можно ли обойтись без какой-либо системы, заменив ее сотрудниками охранного предприятия?
– СКУД однозначно нужна, и мы уже полностью ушли от замков и ключей. Видеонаблюдение тоже нужно. А вот биометрию не используем, пока нет необходимости. Охрана периметра – да, но у нас комбинированный подход, с обходами.
Очень многие производители делают свои системы закрытыми, автономными, а мы хотим ту же СКУД интегрировать с учетными системами, связать получение отчетов и уведомления с Telegram. Мы активно работаем в этом направлении, такие стыки технологий для внутреннего пользования позволяют очень облегчить нам жизнь. Например, если в штате есть сотрудник, который работает с девяти утра до шести вечера, но по каким-то причинам он приходит на работу в восемь часов вечера, с одной стороны, можно поставить запор на СКУД и проход не откроется, а с другой – можно проход разрешить и сделать моментальное уведомление в Telegram начальнику охраны и руководителю отдела о том, что был проход на рабочее место. Именно такие связки технологий/систем мы и разрабатываем.

– Есть ли у вас сложности с выбором поставщиков оборудования?
– Как бы парадоксально это ни звучало, но даже при наличии денег не всегда все можно купить.
Во-первых, встает вопрос лицензирования. Если в оборудовании есть чипы или алгоритмы шифрования, они в обязательном порядке должны получить лицензию. По-другому привезти и использовать оборудование никак нельзя.
Следующий момент – это дефицит. Во время пандемии выросли сроки поставок на многих заводах.
Мы уже пришли к тому, что цена не является основным критерием при выборе. Цена услуг любого рода должна быть "в рынке". Мы уже "наелись" самого дешевого, что есть в доступе, но ломается, и с этим потом ничего нельзя сделать. По закону о защите прав потребителя, если такой продукт купило физлицо, то в течение 14 дней можно потребовать замену, возврат либо ремонт, да и то, если компания еще существует. По закону для юрлиц такого нет: при поломке оборудование берут в ремонт, проходит полгода, а они все еще ремонтируют.
Цена на рынке обусловлена сервисом, и здорово, когда поставщик готов забрать оборудование, которое вышло из строя, дать временную подмену или полностью заменить на новое. И здесь в первую очередь важны надежность, лояльность и адекватность поставщика. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Технологии ритейла: "о дивный новый мир"

Любой потребительский рынок крайне чувствителен к изменениям в технологиях, и ритейл как передовой край B2C наиболее восприимчив ко всему новому. Даже самые низовые сегменты быстро добавляют свежие инструменты: например, в 2005 г. все точки Подмосковья, от торговли дровами до шашлычных, оперативно обзавелись яркими световыми коробами. Отставать от конкурентов нельзя



Евгений Добринин

Коммерческий директор "Навиком" – эксклюзивного представителя Garmin в России

Цивилизованный ритейл непрерывно бегает в рамках одного и того же цикла: сокращение пользовательского внимания – дефицит времени на принятие решения и покупку – отвлечение на альтернативы или другие занятия. Эти ограничения и определяют главную задачу любой розничной торговли – повышение эффективности, упрощение покупки, ускорение закрытия сделки. На технологическом уровне речь идет о переходе к практически бесшовным решениям.

В онлайне ушли в прошлое времена, когда вы делали заказ через электронную переписку – сейчас большинство магазинов позволяют делать покупки в несколько кликов и без регистрации. В живой рознице все идет к тому, что магазин сам обслужит вас: подскажет, куда идти в зале, примерит на вас товар и примет платежи.

E-com: гипермаркет в вашем кармане

Интернет-магазин стал очень компактным: согласно данным SimiCart, к 2021 г. доля покупок через мобильные устройства в электронной коммерции достигла 73%. Прямое следствие – миниатюризация поисковых интерфейсов, корзин, карточек товаров.

У вас больше нет возможности показывать клиенту 10 товаров на широком экране, и вы вынуждены показывать ему 1–2. Значит, на "да/нет" нужно предлагать самую высоковероятную покупку. Именно поэтому одним из значимых трендов является кастомизация ассортимента, развитие предиктивных и подсказывающих систем, машинное обучение и ИИ. Метки вида cookie, привычные нам с конца 1990-х гг., дополнились UTM-метками, пиксельными счетчиками, регистрациями в сквозных сервисах и экосистемах, накапливающих большие массивы данных о самом потребителе, его вкусах, предпочтениях и поведении.

Альтернативы находятся в одном клике, поэтому потеря клиента крайне болезненна и довольно вероятна: по статистике, в мире доля брошенных корзин в интернет-магазинах превышает 75%. Если покупатель все же ушел, существует масса способов его вернуть: "Однажды ты спросишь меня: кого я люблю больше, тебя или маркетинг? Я отвечу, что маркетинг, и ты уйдешь... Но вернешься, потому что ретаргетинг, автоворонка, программа лояльности". В этой шутке доля шутки совсем невелика.

Набор решений, которые внедряет e-com, в целом сводится к 10 позициям:

1. Упрощение процесса покупки.
2. Подогревающие эффекты (дефицит и срочность).
3. Множество вариантов оплаты.
4. Добавление кредитных продуктов и рассрочек.
5. Прозрачность ценообразования и понятность тарифов на доставку.
6. Использование виртуальных стимулов, удерживающих покупателя в процессе.
7. Работа с возвратами.
8. Дополняющие товары и наборы.
9. Расширенное информирование в форме сторителлинга.
10. Геймификация.

Все эти эффекты относятся либо к организации бизнеса, либо к маркетингу, но их конверсия напрямую зависит от технологической обвязки конкретного магазина. Фокус на бесплатную доставку можно сделать при определенном геотаргетинге, а предложение по покупке в рассрочку – клиенту, недавно заполнявшему заявку на кредитную карту в банке-партнере.

Офлайн: все крутится вокруг вас

Если пластичность цифровых решений не удивляет, то метаморфозы, происходящие в живом, физическом мире, поистине впечатляют. Благодаря решениям вида Amazon Go мы скоро забудем о кассирах, Amazon Palm снимет проблему забывчивости: оставить дома кредитку можно, но ваша рука и радужная оболочка всегда с вами.

Всего 10 лет назад ситуация была совсем иной. Возможности для персонифицированной навигации в магазине или кастомизированного предложения были практически нулевыми. Сегодня распространение цифровых поверхностей в сочетании с комплексами, отслеживающими поведение потребителя, позволяет менять магазин лично для него.

Работает это примерно так: если человек, находясь в магазине, пошел в зону зимних товаров и долгое время там находился, разглядывая лыжи, санки, коньки, мы можем зафиксировать время его пребывания в этой зоне и контент, который интересен этому человеку. Собранная информация обрабатывается и используется в следующей точке касания. Если человек проследовал в отдел обуви, есть смысл показывать ему рекламу зимней обуви или даже конкретных спортивных брендов, поскольку мы выяснили, что он интересуется зимними активными видами спорта, вывести на экран указатель, направляющий в нужный отдел.

Подобные решения идеально встраиваются в бескассовые магазины. Решения, подобные франшизе Briskly, создают интегрированную среду, которая обеспечивает и учет товаров, и их идентификацию в корзине покупателя, и оплату. Доступность RFID-меток позволяет наносить их на небольшие товары и мгновенно показывать вам как пречек, так и рекомендации по дополнительным покупкам.

Отсутствие очереди – еще один фактор конкурентоспособности, учитывая, что 86% американцев отказываются от покупок, если приходится долго ждать обслуживания, а в России лояльность к магазину у человека снижается в среднем на 7-й минуте пребывания в очереди, а спустя 10 минут он просто уходит.

Конвергенция и омниканальность

Фантасты начала XX века о таком могли только мечтать, но сегодня магазин может "узнать" вас, даже если вы в нем никогда не были. Достаточно хоть раз сделать с мобильного телефона покупку в интернет-магазине, подключившись к общественному Wi-Fi в кафе или метро.

Система запомнит ваш MAC-адрес и по прибытии в магазин поприветствует вас, сразу предложит товары, которые вам оптимально подходят. Сервисы, подобные Upmetric, помогают идентифицировать покупателей, объединить данные об офлайн-покупках потребителя с его онлайн-данными, персонализировать рекламу, основываясь на истории всех покупок, и в конечном итоге повысить ROI и другие метрики.

Сквозная аналитика позволяет понять источник знаний о магазине: впервые собственники торговых точек способны ответить на вопрос "Откуда о нас узнали?", не обращаясь к клиенту. Вы можете достаточно уверенно понять, что привело клиента – вывеска, выгодное расположение на первой линии или упоминание в публикации, СМИ, рекламе.

Автоматическая идентификация предполагает включение покупателя в различные программы лояльности как самого ритейлера, так и партнеров и настройку будущих рекламных каналов, чтобы помочь потребителю остаться с брендом: покупателю тура на горнолыжный курорт показать рекламу лыж и ботинок, а билета до Сочи – крем от загара и плавки. ■

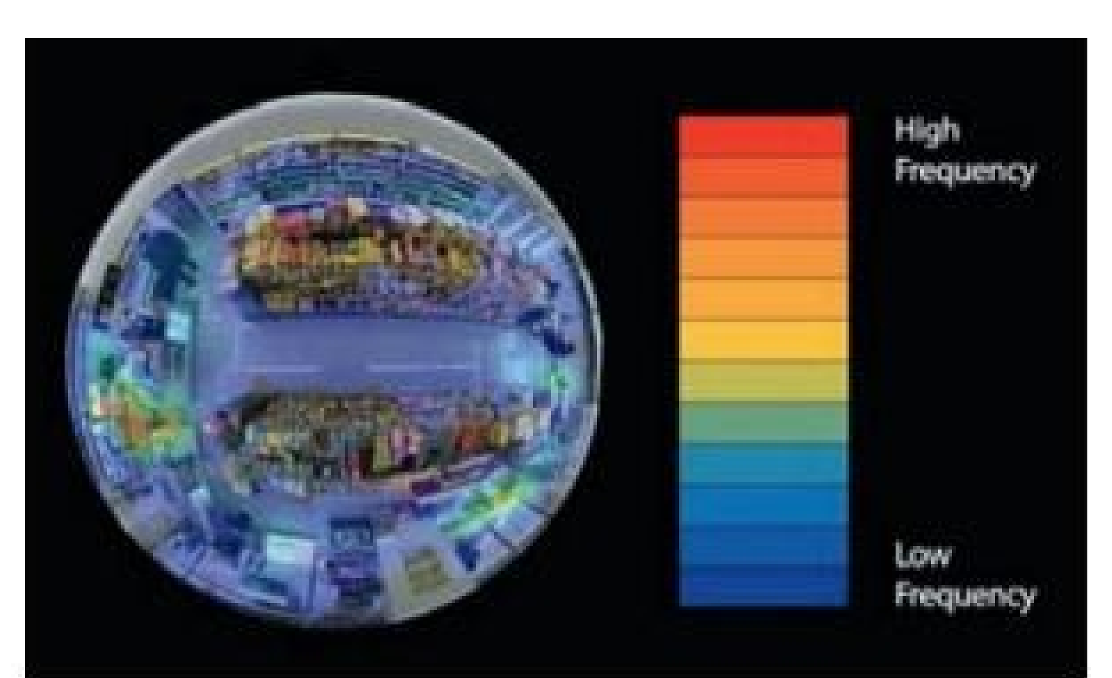
Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Fisheye IP-камера WISENET QNF-9010 – панорамный обзор на 360 градусов и встроенная видеоаналитика для ритейла

Представляет "АРМО-Системы" www.armosystems.ru







Производитель
Hanwha Techwin, www.hanwha-security.com

Реклама

Появление на рынке	Сентябрь 2020 г.
Ценовой сегмент	Низкий/средний

Уникальные преимущества

Реализация на собственном чипсете Wisenet. Разработка не с нуля, а с учетом предшествующих наработок вендора в этом сегменте. Данная модель – последовательное продолжение развития функционала Fisheye-камер Wisenet.

Новый подход к решению задач

Организация видеонаблюдения в непростых условиях торгового зала со специфическим интерьером, стеллажами и множеством "слепых" зон. Установка панорамной камеры решает сразу несколько задач видеосистемы, при этом снижается количество требуемых камер на объекте. Бизнес-аналитика встроена в камеры.

Технические особенности

- Разрешение 12 Мпкс.
- Расширенный динамический диапазон (WDR 120 дБ).
- Дополнительный аналоговый видеовыход.

Экономическая эффективность

Установка всего одной камеры помогает оценить эффективность работы магазина. Видеоаналитика (подсчет посетителей, составление тепловой карты и др.) встроена в камеру и не лицензируется, не требует использования мощных серверов. Полнофункциональное решение Wisenet из демократичной серии Q, а не дорогой X. Камера корейского производителя с подтвержденным качеством, по цене сопоставимая с китайскими аналогами. ■

Проекты
Розничные торговые предприятия

см. стр. 120 "Ньюсмейкеры"

Id-Target – биометрический программный продукт для персонализированного взаимодействия с покупателями

Представляет "РекФэйсис" www.recfaces.com







Реклама

Появление на рынке	Июнь 2020 г.
Ценовой сегмент	Средний и высокий

Уникальные преимущества

Id-Target – готовый продукт для обогащения систем видеонаблюдения розничных площадок функционалом лицевой биометрии, способный стать единым инструментом для повышения лояльности клиентов, расширения блоков продаж и маркетинга по анализу данных о посетителях, а также решения задач служб безопасности.

Конкурентные преимущества

Id-Target – это законченный коробочный продукт, который разворачивается за 20 минут, имеет открытый API для интеграции с CRM-системами, а качественный уровень технической поддержки и обновлений решения уже оценен международными клиентами.

Новый подход к решению задач

Идентифицируйте постоянных покупателей и определяйте количество уникальных. Пол, возраст, возвратность и период возврата – Id-Target покажет динамику изменения этих показателей и сформирует отчеты, а идентификация по "черным спискам" закроет вопрос борьбы с магазинными ворами.

Технические особенности

- В Id-Target предусмотрена технологическая возможность использования как на централизованных объектах, так и на территориально распределенных, что особенно актуально для торговых сетей.
- Архитектура продукта Id-Target позволяет шифровать и деперсонализировать данные, обеспечивая высокий уровень безопасности их хранения и передачи внутри контура решения.
- Система способна идентифицировать посетителя в медицинской маске.

Экономическая эффективность

- Упрощает и таргетирует взаимодействие с покупателем.
- Повышает конверсию предложений и уровень Up-Sales продаж.
- Минимизирует потери от магазинных краж. ■

Потребители
Ритейл среднего и высокого ценового сегмента

Проект
Ельцин Центр

см. стр. 120 "Ньюсмейкеры"

Облачная IP-камера CD330: испытано, надежно

Представляет Camdrive www.camdrive.ru



Потребители
Магазины, дома, квартиры, небольшие склады

Уникальные преимущества

В отличие от стандартных камер, CD330 позволяет развернуть систему безопасности. Детекция движения реагирует исключительно на живые объекты, а не на изменение освещенности, смену погодных условий или движение листвы при порывах ветра.

Появление на рынке	II квартал 2020 г.
Ценовой сегмент	Средний

Новый подход к решению задач

IP-камера CD330 обладает расширенными возможностями идентификации несанкционированных действий вне зависимости от уровня освещенности на объекте. Встроенный PIR-датчик (пироэлектрический инфракрасный) реагирует на тепловое излучение и позволяет безошибочно обнаружить движение в контролируемой зоне. Будьте в курсе происходящих событий! Вовремя получайте извещение и видео-/аудиоинформацию в момент события.

Технические особенности

1. Встроенный модуль Wi-Fi стандарта IEEE 802.11 b/g/n.
2. Встроенный в IP-камеру активный микрофон с акустической дальностью до 10 м.

Экономическая эффективность

Вместо двух разных устройств из разных направлений безопасности – видеонаблюдения и теплового датчика используется одно, ведущее запись в облако. Это исключает необходимость наличия сервера или NVR на объекте. ■

см. стр. 120 "Ньюсмейкеры"

MotionCam – датчик движения с фотокамерой для верификации тревог

Представляет Ajax Systems www.ajax.systems/ru





Появление на рынке	2020 г.
Ценовой сегмент	Средний

Главное назначение

MotionCam от Ajax Systems – это беспроводной датчик движения с фотокамерой для подтверждения тревог. Он решает проблему выезда охранных патрулей по ложным срабатываниям. Зафиксировав движение, MotionCam делает серию фотографий для оценки ситуации. Таким образом, владельцы системы и охранная компания видят, действительно ли произошло вторжение или систему забыли снять с охраны по неосторожности.

Технические особенности

При передаче изображений по радиосвязи не уменьшилась дальность связи MotionCam. Как и другие датчики движения Ajax, он работает на расстоянии до 1700 м от хаба. Это один из лучших показателей для охранных устройств с камерами.

Конкурентные преимущества

У MotionCam рекордная автономность для охранных датчиков с камерами – до 4 лет работы от комплектных батарей. Причем это не оптимистичный прогноз при идеальных условиях, а расчет времени работы при типичном использовании, с учетом перепадов температуры и периодических срабатываний.

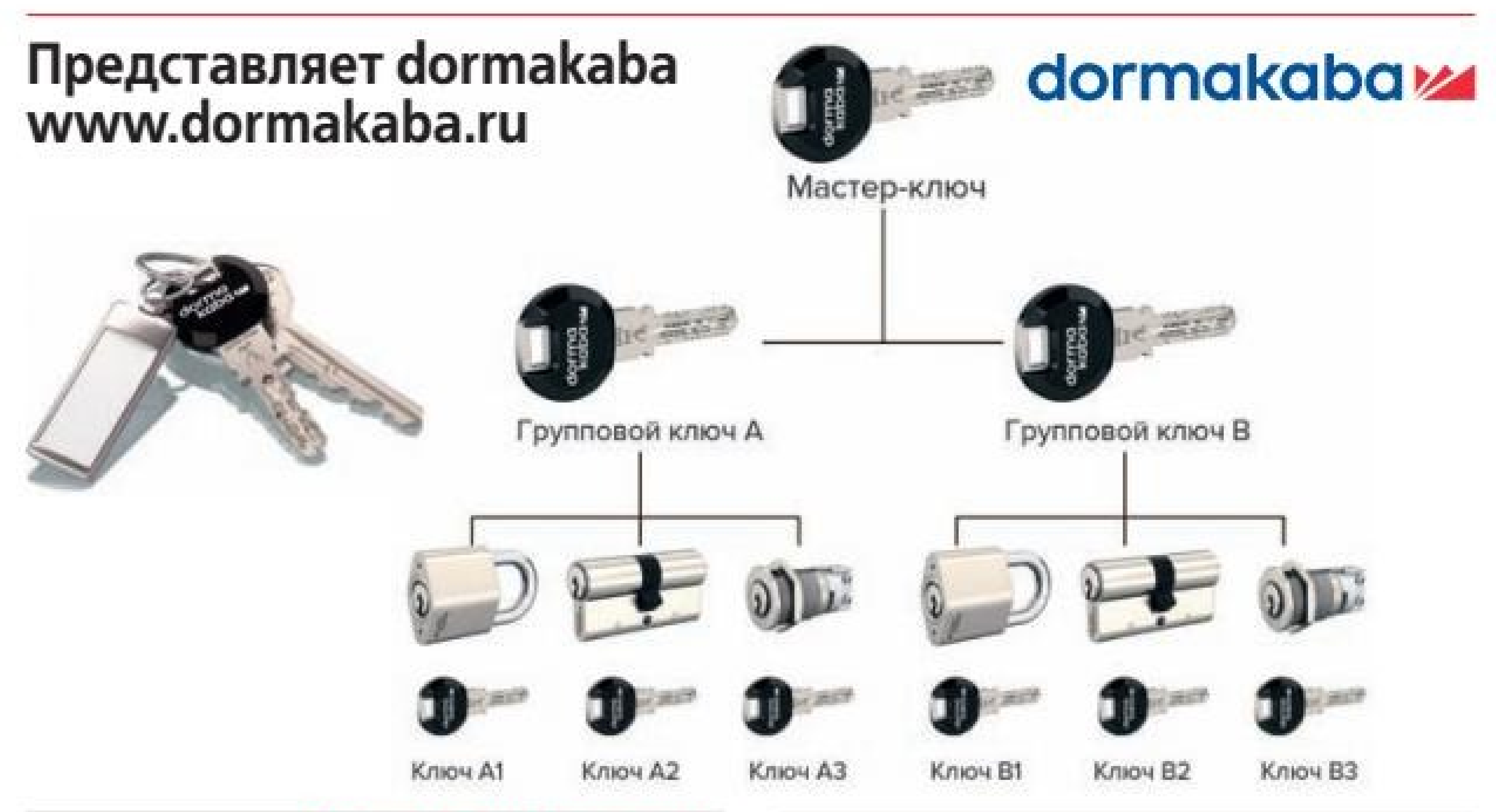
Приватность и безопасность

Разработчики MotionCam позаботились о приватности. Датчик активирует камеру только при тревоге – ни у пользователей, ни у охранной компании нет лазейки, позволяющей датчику сделать фото по запросу. Все снимки защищены шифрованием на каждом этапе передачи и во время хранения на сервере Ajax Cloud, аналогично истории событий системы безопасности. Никто не обрабатывает и не анализирует фото с объектов пользователей. ■

см. стр. 120 "Ньюсмейкеры"

Системы "Мастер-ключ" для безопасного доступа в магазины

Представляет dormakaba www.dormakaba.ru



Главное назначение

Компания dormakaba, имея огромный опыт в области производства систем безопасности, занимается в том числе и таким видом продукции, как мастер-системы на механических цилиндровых механизмах с ключами. Они очень удобны в использовании, экономичны и позволяют организовывать контроль доступа именно так, как этого требует высшее руководство или служба безопасности компании.

Появление на рынке	2001 г.
Ценовой сегмент	Средний и высокий

Конкурентные преимущества

Мастер-системы dormakaba применимы во всех областях деятельности и на любых объектах, начиная от небольшого загородного дома с несколькими дверями и заканчивая большим производством или бизнес-центром с количеством дверей 5000 и более.

Мастер-системы эффективны и в сетевых структурах, например в сетевом ритейле. Наша компания может предложить создание как небольшой мастер-системы для одного магазина, так и единой системы ключей для сети магазинов и офиса. Больше не нужно иметь большие связки ключей и следить за тем, кому какой ключ выдается.

Технические особенности

Всех сотрудников организации можно разделить на группы согласно требованиям безопасности или уровню доступа, тем самым разграничив его: управляющий магазином имеет доступ ко всем дверям, у продавцов есть доступ к торговому залу и складу, у уборщиц и техников – к торговому залу и техническим помещениям, у экспедиторов – к зоне разгрузки и складу. И таких магазинов может быть несколько. У генерального директора и, например, начальника службы безопасности есть мастер-ключ, который может открыть все двери всех магазинов, офиса и т.д.

Экономическая эффективность

Наши возможности по созданию мастер-систем безграничны, а различные модели цилиндров и дополнительные опции способны удовлетворить требования любого заказчика. ■

см. стр. 120 "Ньюсмейкеры"



Константин Сергеев

Директор по безопасности ТС "Монетка", преподаватель курса "Корпоративная безопасность" УрГЭУ, руководитель объединения "Союз руководителей служб безопасности бизнеса", член Общественного совета МВД России по г. Екатеринбургу

Покупательская корзинка как сигнал о краже в магазине

Магазинная кража (шоплифтинг) – это тайное хищение товаров из магазина. Помочь выявить его может покупательская корзина. Как одна из контрольных точек, включенных в систему мероприятий по предотвращению товарных потерь, сама корзинка или ее отсутствие могут дать сигнал о происшествии. Покупательские корзины, которые есть практически в каждом продуктовом магазине, – это не только удобное средство для совершения покупок посетителями, но и один из атрибутов для совершения кражи магазинными ворами

На начало 2021 г. в Российской Федерации административная ответственность за кражу наступает с 16 лет, уголовная ответственность – с 14 лет. Административная ответственность (мелкое хищение) предусмотрена ст. 7.27 АК РФ:

- 1 часть. Мелкое хищение чужого имущества, стоимость которого не превышает 1000 рублей;
- 2 часть. Мелкое хищение чужого имущества стоимостью более 1000 рублей, но не более 2500 рублей.

За повторное мелкое хищение подвергнутым ранее административному наказанию по ч. 2 ст. 7.27 УК РФ предусмотрена ст. 158.1 УК РФ.

Уголовная ответственность за хищение (кражу) предусмотрена по ст. 158 УК РФ – хищение чужого имущества стоимостью более 2500 рублей.

Контрольная точка № 1. Корзинка, оставленная в торговом зале

В 2018 г. в кинопрокат вышел фильм японского режиссера Хирокадзу Корээда "Магазинные воришки". Фильм вызвал живой интерес публики и получил множество наград, в том числе главный приз Каннского кинофестиваля, и даже был номинирован на "Оскар" как лучший фильм на иностранном языке. Если исключить смысл, заложенный режиссером в драматургию картины, и посмотреть на фильм глазами специалиста по предотвращению товарных потерь в ритейле, можно увидеть ряд интересных злободневных сцен.

Одна из них – в самом начале фильма, когда отец с сыном крадут в супермаркете продукты, складывая их в рюкзак. После хищения в магазине остается корзинка с продуктами, которая бралась для прикрытия.

Итак, в торговом зале осталась корзина с товаром. Может ли это быть сигналом о хищении? Сколько таких корзинок за день остается во вверенном вам магазине? Ретроспективный видеоконтроль подобных фактов включен в вашу систему профилактики краж?

С вводом процедуры обязательного просмотра системы видеонаблюдения при выявлении факта оставленной в торговом зале корзинки торговые сети стали фиксировать лица людей, совершивших хищение, и затем осуществлять персонализированную профилактику рецидивных краж.

Контрольная точка № 2. Недостача корзинки

Большинство российских магазинов формата "дискаунтер" (площадью от 200 до 1500 кв. м) отказались от стационарных постов охраны и антикражных систем, доверив функцию "первого поста" (контроля кассовой линии и входной группы) персоналу торгового зала и системам видеонаблюдения.

Основную часть хищений в магазинах злоумышленники совершают с помощью личных вещей (сумки и рюкзаки, потайные карманы, капюшоны, коляски и т.д.). Тем не менее вынос товаров в покупательской корзинке не редкость. Зачастую в этом случае кражи не только рецидивные, но и групповые. Шоплифтеры перемещаются между магазинами на личных автомобилях или такси, не посвящая, как правило, водителя такси в свои преступные намерения. Выносят товар большими объемами, используя корзинки.

Соответственно, помимо недостачи товара, образуется и недостача корзинки (которая, не будем забывать, тоже имеет цену и увеличивает сумму ущерба). Так, один "шоплифтер-математик" (категория шоплифтеров, совершающих хищения на сумму не выше предусмотренной ответственностью КоАП) поплатился тем, что, рассчитав стоимость похищаемого товара, не учел стоимость корзинки и получил ст. 158 УК РФ.

Отсутствие корзинки – это сигнал к просмотру архива видеонаблюдения. Но чтобы понять, что корзинка в недостаче, нужно закрепить соответствующие контрольные процедуры. Согласитесь, каждый день после закрытия магазина считать корзинки – не самое эффективное (и не самое привлекательное) занятие для персонала. Возможный вариант решения: определенное стандартом количество корзинок торгового зала занимает определенную высоту и отмечается линией в отведенном месте размещения корзинок (как правило, на входе в торговый зал). Если после закрытия магазина корзинок не хватает, это будет заметно. Задача персонала в таком случае – проверить еще раз торговые помещения и, если недостача подтвердится, уведомить специалиста по безопасности. Последний, в свою очередь, просмотрит видеоархив, зафиксирует факт кражи и подготовит заявление в полицию, попутно поставив лица нарушителей на видеоконтроль.

Помощь видеоаналитики

Созданию доказательной базы, направленной на быстрое и полное раскрытие преступлений и дальнейшую профилактику хищений, способствует современная видеоаналитика. Так, благодаря информационно-аналитической системе "СТОП Шоплифтер" была выявлена не одна группа магазинных воров. Ярким событием стало выявление в Екатеринбурге этнической организованной преступной группы, получившей название "Выйти на линию" и промышляющей кражами из магазинов. Дело было поставлено на поток: злоумышленники располагали автомобилями для мобильности, складами для хранения похищенного и точками сбыта. Свою "будничную работу" по хищению товаров они между собой называли "выходом на линию". Задержание группы проводили сотрудники отдела по борьбе с организованной преступностью управления уголовного розыска ГУ МВД России и СОБР прямо в магазине, куда преступники пришли на очередное дело.

Отдельно стоит сказать о категории "шоплифтеров-футболистов", которые перемещают наполненную товарами корзинку по полу к двери ногой, стараясь таким образом скрыть подготовку к краже от глаз персонала и совершить тайное хищение, дождавшись удобного момента.

Необходимо, но недостаточно

Безусловно, контрольные мероприятия с корзинкой не закрывают всех вопросов сохранности товаров. Но при этом они просты, доступны, не требуют особых затрат сил и средств и потому имеют место в арсенале специалиста по безопасности ритейла. ■

Источник: www.ekb-security.ru

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Секреты производителей видеонаблюдения

Как отличить рекламу от реальности

Алена Швецова
Независимый эксперт (#cctvMadonna)

Если покупатель не понимает или не чувствует ценности товара или услуги, он будет считать, что все предложения одинаковые, и выберет самый дешевый вариант. Ценность товара или услуги относительна и меняется в зависимости от личного опыта, финансов и реальных потребностей покупателя решить ту или иную задачу

Бренд СВН и его ценность для заказчика

Система IP-видеонаблюдения (далее СВН) включает в себя IP-камеры, структурированную кабельную сеть, коммутаторы, средства записи и хранения видеоинформации (серверы, регистраторы, системы хранения данных), программное обеспечение для администрирования и клиентское (операторское) программное обеспечение. Для расширения функционала СВН применяют аудиоустройства (домофоны, громкоговорители, микрофоны), программную или аппаратную аудио- и видеоаналитику. Часто СВН используют как ядро интегрированной системы безопасности.

Бренды (производители) СВН продают свои решения, чтобы конечный заказчик мог удовлетворить свои потребности, чтобы, в свою очередь, заказчик мог создать и продать свои продукты, услуги и решения своим клиентам.

Чем больше заказчиков и интеграторов знает бренд СВН, тем у него больше шансов стать популярным и продаваемым.

Некоторые бренды видеонаблюдения хотят продать заказчику решение под ключ, некоторые сфокусированы на продаже конкретных компонент (например, только IP-камеры или только программное обеспечение).

Заказчиков СВН условно можно разделить на новаторов (готовы пробовать новые бренды, открыты к экспериментам), традиционалистов (используют то, что популярно) и консерваторов (используют то, что хорошо знают или во что свято верят).

Ценность брендов СВН для заказчиков складывается из двух составляющих: теоретическая часть (читал, слышал, видел) и практическая часть (использовал в реальных проектах, обращался по гарантии, знаю, как работает бренд через 3–5 лет эксплуатации).

Продавая или выводя на рынок бренд СВН, вендоры учитывают портрет потенциальных заказчиков, их тип и опыт взаимодействия с другими брендами.

Знакомство и сотрудничество с брендом СВН

На рынке так много производителей СВН (500+ брендов), что не стоит удивляться, если заказчик и даже системный интегратор не знает их все.

Не стоит поддаваться рекламным слоганам "ведущий мировой производитель", "лидер рынка", "передовой бренд", "популярный производитель" и т.д., лучше познакомиться с рейтингом бренда и внимательно прочитать историю вендора и бренда. Производители – лидеры рынка СВН всегда пишут о своих достижениях в продажах, ссылаясь на свою позицию в конкретном рейтинге.

Рейтинги и ключевые игроки рынка видеонаблюдения

Рейтинг производителей IP-видеонаблюдения определяет статистическое агентство IHS Markit (в прошлом IMS Research) в виде отчета Video Surveillance Market Share Database, который включает производителей IP-камер, видеорегистраторов и VMS (Video Management Software – программное обеспечение для систем управления IP-видеонаблюдением). Отчет IHS Markit Video Surveillance доступен только подписчикам и является платным. Рейтинг компаний в отчете формируется на основании объема продаж и публичной финансовой отчетности компаний.

Смешанный рейтинг производителей систем безопасности формирует также ресурс Asmag на основании объема продаж. Аналитику по мировым рынкам и ключевым игрокам можно найти на ресурсах компаний MarketsandMarkets, Technavio, MarketResearch.com, Mordor Intelligence и т.п.

Ключевыми игроками мирового рынка видеонаблюдения являются: Axis Communications (Швеция), Bosch (Германия), Hikvision (Китай), Dahua (Китай), Hanwha Techwin (Корея), Avigilon (Канада), Pelco (США), FLIR (США), Panasonic (Япония), VIVOTEK (Тайвань), Milestone Systems (Дания), Genetec (Канада), NEC (Япония), Nice (Израиль) и др. Российские вендоры не принимают участия в мировых рейтингах по объемам продаж, так как большинство компаний не показывают публично свою финансовую отчетность.

Знакомство с брендом СВН

С брендами СВН заказчиков знакомят Интернет (доминирующий канал), профильные международные и локальные выставки, системные интеграторы, отраслевые журналы, коллеги и свой собственный практический опыт.

Как происходит знакомство в жизни? Сначала мы встречаемся, знакомимся и слушаем человека. Затем анализируем услышанное, наводим справки о человеке, чтобы принять решение, будем мы с ним сотрудничать или нет. Мы ценим людей за их слова, если они подкреплены реальными делами и конкретными результатами. С брендами и вендорами СВН все точно так же, как в жизни.

Поэтому очень важно качественно и глубоко знакомиться с брендом, поскольку жизненный цикл СВН должен быть не менее 7–10 лет, чтобы заказчик успел получить возврат инвестиций от системы за счет предотвращения инцидентов, снижения экономических и репутационных рисков.

Если существующая СВН не защищает заказчика и не экономит ему деньги, значит, она неправильно спроектирована или выбраны бренды и решения, не соответствующие реальным потребностям заказчика

Очень полезно и интересно знакомиться с историей вендора (производителя) и бренда (то, что продает вендор на рынке конкретной страны под торговыми марками).

Даже если вы знакомы с брендом IP-камер, использовали его в работе, на 100% им довольны и планируете долгосрочную работу с ним, всегда есть смысл оценить его преимущества и риски для ваших проектов:

- проверить актуальный список официальных дистрибьюторов;
- проверить актуальный список авторизованных и сертифицированных интеграторов;
- изучить, что бренд пишет на своем официальном сайте и что о нем пишут в профессиональных новостях;
- познакомиться с актуальной линейкой продуктов и решений, а также оценить, как она изменилась за последний год;
- изучить, как выглядит команда вендора для вашей страны (есть ли офис, сколько человек отвечает за страну) и какую помощь они могут оказать вам и вашей компании в проекте;
- запросить у вендора/дистрибьюторов список успешно реализованных проектов в вашей стране или в мире по вашей отрасли;
- проверить актуальные условия гарантии от вендора и условия, при которых случай будет считаться негарантийным;
- узнать контакты технической поддержки и сервисного центра вендора в своей стране/городе;
- узнать через сайты вендора или официальных дистрибьюторов о предстоящих онлайн- и офлайн-семинарах/вебинарах/ конференциях/выставках на ближайший год и запла-

нировать посещение важных для вас и вашей отрасли мероприятий;
- запланировать прохождение сертификационного технического тренинга для вас и ваших специалистов, чтобы повысить свои компетенции.

Оригинальные, ODM- и OEM-производители IP-камер

Выбор СВН заказчики часто начинают с выбора IP-камер.

Существует огромная разница между оригинальными вендорами и OEM-/ODM-брендами, которую должен понимать каждый интегратор и заказчик.

Оригинальные производители IP-камер

В публичные рейтинги IP-камер (см. раздел "Рейтинги и ключевые игроки рынка видеонаблюдения") попадают только оригинальные производители.

Известно, что революцию в IP-видеонаблюдении в 1996 г. совершила шведская компания Axis Communications. Лидеры рынка аналогового видеонаблюдения того времени Bosch (Германия), Pelco (США), Sony (Япония), Samsung Techwin (Корея), Panasonic (Япония), Sanyo (Япония) и т.п. первую и следующие сетевые камеры Axis восприняли скептически, но спрос со стороны заказчиков и потребность в качественном цифровом видеонаблюдении расставили все на свои места.

К 2006 г. практически у всех производителей аналоговых камер появилась линейка IP, а к 2016 г. на рынке уже полностью доминировали IP-камеры.

До 2010-х гг. заказчики во всем мире, предпочитающие ценность и качество, покупали исключительно европейское и американское оборудование для видеонаблюдения, заказчики, фокусирующиеся на соотношении "цена/качество", покупали японское и корейское оборудование, а заказчики с ограниченным бюджетом покупали тайваньские бренды.

Череда мировых экономических кризисов 2008–2013 гг. (ограниченные бюджеты заказчиков), большие амбиции и весомые финансовые инвестиции (как следствие – агрессивный ценовой демпинг) позволили китайским государственным компаниям Hikvision и Dahua агрессивно выйти на рынок IP-видеонаблюдения, а в 2011 г. Hikvision заняла лидирующую позицию по объему продаж.

С 2010 г. на рынке существует агрессивная конкуренция между китайскими, европейскими, американскими и корейскими производителями (тайваньские компании практически не участвуют в данной гонке). Это постоянная борьба за крупные государственные и частные проекты, это открытие новых заводов в целевых странах, рекламные "войны", открытие представительств, локализация сайтов и инструкций на различные языки, это активная политика привлечения корпоративных заказчиков.

Благодаря оригинальным производителям, которые инвестировали огромные суммы в R&D, процессоры, микроэлектронику и оптику, IP-камеры научились:

- видеть лучше, дальше и больше, чем человеческий глаз;
- формировать четкие и реалистичные цвета при любых сценах;
- видеть в цвете практически в полной темноте;
- видеть сцены при любой контурной и встречной засветке;
- передавать видео и звук;
- взаимодействовать с различными аппаратными устройствами и программным обеспечением;
- за счет мощности процессоров позволили видеоаналитике работать на своем борту;
- получили разнообразие формфакторов и цветов корпусов;
- научились работать в транспорте, в условиях вибрации и повышенных электромагнитных помех;
- слетали в стратосферу, научились работать в условиях жаркой пустыни при +60 °С и арктического холода -60 °С.

За 25 лет своего существования IP-видеонаблюдение прошло путь от 4CIF до 8K и выше. Технологии видеонаблюдения и показатели IP-камер стали лучше, выбор – больше, а цена – меньше, что однозначно способствует выгоде для конечных заказчиков.

Каждый технологический прорыв в IP-видеонаблюдении появлялся благодаря труду самых талантливых инженеров и изобретателей вендоров, которые делали то, что до них ранее не существовало. Однажды мы с вами будем смотреть про это фильмы и сериалы.

OEM- и ODM-производители

OEM (англ. Original Equipment Manufacturer) – это производители оборудования или компонент, которое продается на рынке под другими торговыми марками.

OEM-изделия ориентированы на масс-маркет (бюджетные и низкобюджетные сегменты). Основная страна OEM-производителей – Китай. OEM-производство массовое, характеристики усредненные, ориентированы на неискушенного потребителя решений по видеонаблюдению, которым нужны "просто камеры, чтобы они просто смотрели и просто записывали".

На рынке по поводу OEM существует шутка, что "китайские OEM-производители настолько гибки, что при заказе партии в несколько тысяч камер при желании они на корпусе камеры могут написать даже имя вашего домашнего питомца" или "выпустить партию камер с уникальными серийными номерами для вашего проекта".

ODM (англ. Original Design Manufacturer) – это производители оборудования, которое создается по техническому заданию другой компании и продается на рынке под торговой маркой/брендом компании-заказчика.

Некоторые топовые бренды использовали китайские OEM-/ODM-камеры, а также китайские процессоры для своих бюджетных линеек. Вследствие обнаружения многочисленных критических киберуязвимостей в 2018 г. в США был принят, а с августа 2019 г. введен в действие закон о запрете использования оборудования китайских вендоров Hikvision, Dahua, Huawei, ZTE, Hytera, а также процессоров Huawei Hisilicon в государственных проектах. Поэтому ситуация резко изменилась: большинство брендов отказываются или уже полностью отказались[1] (Bosch, Panasonic, Honeywell) от китайских OEM-/ODM-камер и процессоров Huawei Hisilicon (Axis снял с производства серию Axis Companion Line, Hanwha Techwin перевели некоторые линейки на свои процессоры Wisenet и американские процессоры Ambarella).

Ситуация в видеонаблюдении с OEM/ODM не уникальна, по тому же пути идут торговые дома/торговые сети, часто создавая свой "собственный бренд" бытовой техники.

Учитывая хронический дефицит бюджетов у многих заказчиков на наших рынках на качественные и дорогие решения, китайская OEM-стратегия отлично работает и приносит китайским производителям хорошую прибыль.

Заказчиков, особенно заказчиков с ограниченным бюджетом, легко приучить к "вкусной цене", но где же в такой стратегии заработок вендора? Ведь ему нужно оплачивать труд тысяч своих сотрудников, инвестировать в новые разработки, создавать новые модели, чтобы в дальнейшем не потерять текущих и привлекать новых заказчиков и конкурировать с другими брендами. Демпинг, который начали китайские вендоры в 2010-х гг., постепенно негативно влияет на них самих и снижает их маржу, ведь возникает эффект "дровосека, который рубит сук, на котором сидит".

Сравните сами. В 2012–2013 гг. розничная стоимость топовых IP-камер была порядка 900–1300 долларов (Axis, Bosch), средний сегмент Panasonic и Samsung Techwin (сейчас Hanwha Techwin) в розницу стоил 600–900 долларов, а самыми дешевыми тогда были тайваньские бренды с ценой 400–600 долларов (ACTi, например).

Уже к 2014 г. стоимость топ-брендов снизилась до 700–800 долларов, а нишу самых дешевых IP-камер заняли Hikvision и Dahua с ценой 120–300 долларов.

В 2021 г. стоимость OEM-камер начинается от 50 долларов.

Уже видна тенденция, что китайские вендоры начали конкурировать между собой за заказчиков (например, HiWatch и Hikvision или RVi и Dahua). Чтобы уйти от прямой конкуренции со своими OEM-брендами, Hikvision и Dahua начали создавать более дорогие и сложные решения, а также объяснять своим клиентам ценность, то есть делать то, что европейские, американские и корейские бренды делали всегда для своих заказчиков.

Бренды VMS и видеоаналитики

В проектах можно встретить следующих игроков рынка комплексных решений по VMS (системы управления видеонаблюдением, Video Management System) и видеоаналитике: Axis Communications (Швеция), Bosch (Германия), Hikvision (Китай), Dahua (Китай), Hanwha Techwin (Корея), Avigilon (Канада), Pelco (США), Milestone Systems (Дания), Genetec (Канада), Verint (Израиль), AxxonSoft/ITV (Россия), Trassir (Россия), Macroscop (Россия) и др.

Некоторые из них предлагают комплексные решения под ключ (IP-камеры, VMS, видеоаналитику, контроль доступа, регистраторы/серве-

[1] *https://ipvm.com/reports/bosch-dahua, https://ipvm.com/reports/dahua-oem, https://ipvm.com/reports/honeywell-hides*

ры и т.п.), некоторые фокусируются на разработке VMS и видеоаналитики.

Отдельно на рынке выделяются производители видеоаналитики, профессионально занимающиеся разработкой алгоритмов и созданием решений с использованием машинного обучения и искусственного интеллекта, например распознавания лиц: NEC (Япония), Gemalto (Нидерланды), Ayonix (Япония), Cognitec (Германия), ЦРТ (Россия), NtechLab (Россия), VisionLabs (Россия) и др. Для удобства заказчика в проектах такие решения используются как интегрированные в VMS или в СКУД модули.

Параллельно компаниям, которые разрабатывают свои собственные алгоритмы, растет количество компаний, использующих открытые алгоритмы. Это также влияет на удешевление решений по распознаванию лиц и другой видеоаналитики.

Важно помнить, что система видеонаблюдения корпоративного уровня состоит из IP-камер (15–25% бюджета проекта), программного обеспечения (10–15%), сетевой инфраструктуры (15–20%), но самой значимой по стоимости являются серверы и системы хранения видеоданных (40–60% стоимости проекта). При этом именно VMS отвечает за производительность системы и эффективную работу по обработке и хранению видеоданных[2].

В системе видеонаблюдения корпоративного уровня IP-камеры являются "глазами", VMS – "мозгом", а инфраструктура – "артериями". И если "глаза" сейчас можно подключить через проприетарные протоколы, ONVIF или RTSP практически к любому "мозгу", то различные "мозги" без замены "артерий" пока штатно не совместимы между собой. Часто такие факты удивляют и даже расстраивают заказчиков.

Приведем пример из практики. У заказчика большой холдинг: это сеть АЗС, построенная на базе регистраторов бренда X (500 камер), в головном офисе стоит VMS бренда Y (150 камер), а на отдельном предприятии работает интегрированная система (СВН + СКУД) безопасности бренда Z (300 камер).

Решения по видеонаблюдению строили в разные периоды разные люди. Стоит задача объединить все имеющиеся системы видеонаблюдения, чтобы в центре из одного интерфейса операторам и руководству можно было смотреть все камеры в режиме онлайн и архив, получать тревоги, а также хранить и дублировать в центре записи с некоторых камер 60 дней. И чтобы при этом все действия операторов в системе логировались и было понятно, кто, как и когда сделал экспорт и кто, как и когда отрабатывает тревоги.

Звучит просто, но на практике это сложная техническая задача, и интегратору нужно потрудиться, чтобы ее решить, потому что нужно проверить совместимость VMS бренда Y и бренда Z, понять, могут ли они работать с архивами регистраторов бренда X, проверить каналы, уточнить, могут ли камеры на местах выдать второй/третий поток в полном разрешении без потери качества и т.п. На практике VMS различных вендоров не совместимы друг с другом, так как каждый производитель по-разному работает с архивами. Часто доступ к архиву является камнем преткновения, чтобы работать с архивом NVR, его нужно интегрировать в VMS. Если это одно устройство – не проблема, а если это 20–50 различных моделей NVR с разными прошивками, то задача становится сложной, с множеством точек отказа.

Лучшим техническим вариантом решения данной задачи на 950 камер будет приведение всех трех систем к единой VMS, создание иерархии, подключение всех систем как подчиненных, создание правил, расписаний, уровней доступа для руководства и сотрудников. Решение такой задачи потребует финансовых и человеческих ресурсов, но успешный результат действительно повысит ценность системы видеонаблюдения для заказчика, потому что он сможет управлять единой системой, расширять функционал и добавить видеоаналитику в будущем, контролировать инциденты и т.п.

Чтобы заказчик получил решение своей глобальной задачи и достиг поставленных целей, важно до момента покупки и внедрения решения убедиться, что все компоненты, устройства и подсистемы смогут эффективно работать друг с другом, а функционал системы может быть расширен в будущем.

Как проверить возможности бренда на практике

Все вендоры описывают функциональные возможности своих продуктов в Datasheets (спецификациях). Казалось бы, открывай и читай. Но желание продать заказчику свои камеры любой ценой и рекламные "войны" привели к тому, что бюджетные производители пишут в спецификациях что угодно (например, светочувствительность 0,001 лк или WDR 120 дБ при стоимости камеры в 50–100 долларов), ведь их за это никто не накажет. Получается, что на бумаге все IP-камеры хороши. При такой ситуации немудрено, что заказчик без практического опыта выбирает самые дешевые IP-камеры, ведь "зачем платить больше", если в доступной по цене камере "лучшие" показатели и даже встроенная "видеоаналитика".

Наиболее частой просьбой заказчика к интегратору (а далее интегратора к дистрибьютору или вендору) является "покажите мне сравнение бренда А и Б между собой". Это простая просьба заказчика на практике является сложновыполнимой. Почему? Потому что в странах СНГ не существует независимой организации, не связанной с разработкой программного или аппаратного обеспечения, которая бы объективно и незаангажированно проводила сравнительные тесты оборудования и решений между собой. Сертификация оборудования на соответствие тем или иным стандартам не дает ответ на вопрос "Как выбрать и что для меня будет лучше?". Существует много "экспертов" по распаковке и демонстрации продуктов, существуют профессиональные статьи или видеосравнения, но пока ни один наш ресурс не может претендовать на 100%-ную объективность.

Производители IP-камер и решений по видеонаблюдению, конечно, проводят внутреннее сравнение собственных продуктов с конкурентами. Но из-за профессиональной этики эти сравнения не предоставляются ни дистрибьюторам, ни интеграторам, ни тем более заказчикам. И если для камер можно выполнить сравнение "лоб в лоб" по спецификации, то функционал различных производителей VMS и видеоаналитики описан так, как удобно вендору, а иногда даже скрыт из публичных ресурсов.

Кто-нибудь делает объективные сравнения? Да, делает. Независимым и объективным источником информации по IP-камерам, программному обеспечению, видеоаналитике и контролю доступу является американский ресурс IPVM. Он существует на деньги своих подписчиков и доступен по всему миру, среди них и сами вендоры, и интеграторы, и, конечно, заказчики. Годовая подписка стоит от 199 до 1349 долларов за индивидуальный доступ, что приемлемо для всех, кто считает себя профессионалами на рынке видеонаблюдения и систем безопасности.

Именно IPVM делает то, что чаще всего спрашивают наши заказчики и интеграторы, – проводит свои собственные сравнительные тестирования вендоров и моделей между собой, проверяет заявленный функционал (разбирает по косточкам) и раскапывает скрытые за рекламными брошюрами функциональные детали и возможности. Поскольку IPVM по-настоящему независим от производителей и не вовлечен в рекламные кампании, компания занимает довольно жесткую и принципиальную позицию по отношению ко всем вендорам на рынке, и часто вендоры боятся их статей, потому что время от времени "прилетает" даже известным и уважаемым на рынке брендам. Единственное неудобство ресурса в том, что он публикует материалы только на английском.

А как же мне в моей стране проверить/сравнить оборудование и решение? Объективным способом проверки заявленного в спецификации функционала IP-камер, NVR, VMS и видеоаналитики является сравнительное тестирование (делает интегратор на своей площадке) или пилотный проект (делает интегратор или заказчик на объекте заказчика[3]). Да, это требует времени и ресурсов, но зато на 100% гарантирует заказчику, что ему не продадут кота в мешке.

Сравнительное тестирование и пилот позволят интегратору и заказчику:

- отделить рекламу от реальности;
- более точно сформулировать задачу проекта;
- получить объективные факты, какое именно оборудование и за какие деньги решит те или иные задачи заказчика;
- получить свой собственный опыт с различным оборудованием;
- проверить сценарии и логику работы системы (камеры + VMS + видеоаналитика);
- сформировать для себя практическую ценность брендов.

Понимая практическую ценность бренда, его стоимость, текущие и будущие задачи, легко сделать правильный выбор для проекта любого уровня. ■

[2] Швецова А. Дешевле или дороже? Совокупная стоимость владения или TCO систем видеонаблюдения // Системы безопасности. 2020. № 5. С. 55–59.

[3] Швецова А. Как пилотный проект по видеонаблюдению поможет интегратору выиграть, а заказчику – получить работающее решение // Системы безопасности. 2020. № 5. С. 55–59.

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Транспортная безопасность – сформировавшийся юридический институт

С прошлого года Иван Тушко стал постоянным автором нашего журнала. Сфера его компетенции – транспортная безопасность. Иван закончил Дальневосточный университет путей сообщения, затем получил еще два высших образования, имеет квалификацию экономиста, степень магистра юриспруденции и 10-летний опыт в сфере транспортной безопасности. Работал во ФГУП "ЗащитаИнфоТранс" Министерства транспорта Российской Федерации, ГУП "Петербургский метрополитен", занимался проектами в сфере антитеррористической защищенности на Дальнем Востоке, Сибири и западных регионах страны. Настоящее место работы – СПб ГУП "Пассажиравтотранс". В этом интервью Иван делится своим мнением по актуальным вопросам транспортной безопасности



Иван Тушко

Специалист-эксперт в области обеспечения транспортной безопасности, магистр юриспруденции

– Иван, какие риски вы считаете системно значимыми для предприятий транспортной отрасли?

– Для любого транспортного предприятия одной из наиболее острых проблем является низкая эффективность исполнения обязательных требований законодательства в области транспортной безопасности. На проведение различных организационных мероприятий, оснащение объектов транспорта инженерно-техническими средствами расходуются значительные финансовые средства, но все это не дает абсолютной гарантии в обеспечении полной защиты транспортного комплекса и пассажиров.

При этом некоторые требования законодательства являются избыточными, не учитывают специфику конкретного вида транспорта, технологический процесс конкретного типа объекта транспорта, однако за их неисполнение предусмотрена административная ответственность с существенными штрафами и даже приостановкой деятельности предприятий.

При интенсивном пассажиропотоке (к примеру, в метро) эффективность проведения досмотровых мероприятий резко снижается и не может обеспечить такой же контроль за выявлением нарушителей и запрещенных предметов и веществ, как в аэропортах.

На государственном уровне отсутствует научно-практическая программа или методика, на основании которых было бы возможно провести обоснование установления границ зоны транспортной безопасности и мест размещения КПП для каждого типа объекта. В различных регионах страны методы и способы обоснования установления границ зоны транспортной безопасности могут существенно отличаться друг от друга.

Отдельного внимания требует вопрос гармонизации законодательства в сфере аттестации сил обеспечения транспортной безопасности и трудового законодательства.

– Какие задачи в сфере транспортной безопасности являются приоритетными?

– Федеральный закон от 09.02.2007 г. № 16-ФЗ "О транспортной безопасности" провозглашает шесть основных задач обеспечения транспортной безопасности:

1) нормативное правовое регулирование в области обеспечения транспортной безопасности;

2) определение угроз совершения актов незаконного вмешательства;

3) оценка уязвимости объектов транспортной инфраструктуры и транспортных средств;

4) категорирование объектов транспортной инфраструктуры и транспортных средств;

5) разработка и реализация требований по обеспечению транспортной безопасности;

6) разработка и реализация мер по обеспечению транспортной безопасности.

В сложившейся обстановке основные задачи обеспечения транспортной безопасности, обозначенные государством, остаются неизменными. В то же время требуется уделить особое внимание актуализации перечня угроз совершения актов незаконного вмешательства, с учетом развития информационных технологий, совершенствования инженерных и технических средств, применяемых потенциальными нарушителями.

Одной из наиболее острых проблем является низкая эффективность исполнения обязательных требований законодательства в области транспортной безопасности. На проведение различных организационных мероприятий, оснащение объектов транспорта инженерно-техническими средствами расходуются значительные финансовые средства, но это не дает гарантий в обеспечении полной защиты транспортного комплекса и пассажиров

После данной актуализации можно будет говорить о корректировке остальных задач в целях соответствия системы применяемых мер по антитеррористической защищенности реальным действующим угрозам.

Обеспечение транспортной безопасности транспортного комплекса от потенциальных внутренних и внешних угроз несанкционированного вмешательства в его деятельность имеет важное стратегическое значение для государства.

Транспортная инфраструктура всегда будет привлекательной мишенью террористических атак

в связи с наличием высокой концентрации человеческих ресурсов и возможностью причинения вреда жизни и здоровью людей, нанесения материального ущерба экономике страны, что, как следствие, вызовет необходимый для достижения целей терроризма общественный политический резонанс.

Несмотря на то что с течением времени одни производственные процессы приходят на смену другим, транспорт всегда будет одной из главных отраслей экономики любого государства. Вот почему обеспечение безопасности данного направления будет всегда представлять повышенный интерес.

К сожалению, представители транспортных компаний и специализированных организаций в области обеспечения транспортной безопасности крайне редко привлекаются в качестве экспертов для разработки научно-практических подходов, методик, моделей, стратегий, которые в дальнейшем пополнят нормативную базу и будут носить общеобязательный характер.

– Расскажите, какие конкретные задачи вам приходилось решать в своей профессиональной деятельности.

– Длительный период времени я занимался проведением оценки уязвимости объектов транспортной инфраструктуры (ОТИ) и транспортных средств (ТС). Оценка уязвимости – это определение степени защищенности ОТИ и ТС от угроз совершения актов незаконного вмешательства (АНВ). За период 2011–2020 гг. мною проводилась оценка уязвимости в Дальневосточном, Сибирском, Приволжском, Уральском, Центральном и Северо-Западном федеральных округах России на объектах и транспортных средствах морского, речного, автомобильного, наземного электрического, железнодорожного транспорта и метрополитена.

При разработке документации по оценке уязвимости применялась методика расчета границ зоны транспортной безопасности и критических элементов с учетом ущерба возможных последствий от совершения АНВ, разработанная мною на основе обобщения многолетних работ по оценке уязвимости, а также исследований других ведущих научно-исследовательских учреждений и специализированных организаций. Цель применения данного алгоритма – иметь теоретико-практическое обоснование при определении границ зоны транспортной безопасности и расчете ущерба. Данная разработка показала высокую эффективность на практике, позволила исключить субъективность экспертного мнения и может быть в дальнейшем полезна работникам специализированных организаций.

Степень магистра юриспруденции, по моему убеждению, является безусловным бонусом при работе в отрасли транспортной безопасности, которая перенасыщена различными требованиями законодательства, которые нередко создают коллизии в процессе практического применения.

Во ФГУП "ЗащитаИнфоТранс", ведущем системном интеграторе в области транспортной и информационной безопасности, а также внедрения информационных технологий, я работал сначала в хабаровском, а затем в санкт-петербургском филиале предприятия, получив колоссальный опыт эксперта и руководителя.

В ГУП "Петербургский метрополитен" занимался разработкой системы необходимых мер в области транспортной безопасности и антитеррористической деятельности.

В настоящее время я руковожу отделом транспортной безопасности СПб ГУП "Пассажиравтотранс". Предприятие является одним из крупнейших пассажирских перевозчиков автобусным транспортом Северо-Западного региона России, обслуживает 159 городских и пригородных маршрутов. Ежегодно автобусы перевозят более 300 млн пассажиров. Предприятие имеет 2051 транспортное средство, которые с точки зрения транспортной безопасности по техническим и технологическим характеристикам сформированы в 38 групп. К основным направлениям моей деятельности относится организация пропускного и внутриобъектового режимов, а также организация и контроль за деятельностью предприятия в области обеспечения транспортной безопасности и антитеррористической защищенности.

Несмотря на то что с течением времени одни производственные процессы приходят на смену другим, транспорт всегда будет одной из главных отраслей экономики любого государства. Вот почему обеспечение безопасности данного направления будет всегда представлять повышенный интерес

– Какие пути вы видите наиболее эффективными для повышения собственной квалификации и квалификации сотрудников для обеспечения наивысшего уровня транспортной безопасности?

– Безусловно, ключ к успеху находится в постоянном саморазвитии и поиске путей решения существующих проблем. Мои профессиональные взгляды прямым образом зависят от моих коллег и других знакомых представителей транспортного сообщества, с которыми удается обменяться мнениями на форумах и семинарах. Транспортная безопасность, являясь важнейшей составляющей государственной транспортной политики и частью национальной безопасности страны, за период с 2007 по 2021 г. прошла путь становления и получения обособленности от других профессиональных сфер деятельности, и в настоящее время транспортную безопасность можно рассматривать как сформировавшийся юридический институт.

По моему мнению, большинство мероприятий в области обеспечения транспортной безопасности уже много лет строятся по единому принципу и редко несут в себе нечто принципиально новое. Формат многочасовых лекций, сменяющихся брифингом и рекламными выступлениями компаний-производителей, является устаревшим и изнурительным.

К тому же мы способны усвоить не более 5–10% от общего объема доносимой информации, а это значит, что большинство полезного материала, подготавливаемого спикерами и организаторами, остается невостребованным.

Возможно, выходом из ситуации может стать частичное изменение устоявшегося формата. Тот же брифинг может стать стартом мероприятия, ведь участники пребывают в поисках ответов на практические вопросы и готовы к диалогу. Пандемия коронавируса позволила внести и более кардинальные изменения: онлайн-мероприятия стали вполне логичным решением, охватывающим широкую географию нашей страны. Данный формат создает возможности более широкого привлечения экспертов и снижает затраты для участников.

Я думаю, что путей решения данной проблемы очень много. Главное, чтобы в экспертном сообществе существовала обратная связь, а формат проводимых мероприятий находился в постоянном совершенствовании.

– Какие у вас есть предложения к регуляторам, представителям власти, отраслевым министерствам?

– Комплекс мер, которые принимают государственные структуры для обеспечения транспортной безопасности, далеко не всегда является адекватным, поскольку решения не носят системного характера и чаще направлены на ликвидацию последствий кризисных событий, чем на разработку стратегий и на выявление тенденций. Ощущается явный недостаток научных подходов для анализа ситуаций и применения научно обоснованных методов разработки систем обеспечения транспортной безопасности.

Тенденция последних лет свидетельствует о возросшей потребности в экспертном обеспечении политических решений, расширении консультационной и информационной поддержки государственных политик.

В США и Европе такую экспертную поддержку при формировании политического курса и принятии государственных решений оказывают "мозговые центры" (Think Tanks), которые являются связующим звеном между наукой и политической практикой, их рекомендации основаны на научных разработках, что привносит в процесс принятия решений рационализм, прагматизм и непредвзятость, дистанцированность от идеологических оценок. В России, несмотря на деятельность различных экспертных организаций, их участие в процессе формирования государственных политик пока сравнительно невелико. Многие научные исследования для практиков в нашей стране проводятся высшими учебными заведениями или специально создаваемыми при них научными лабораториями.

Важно привлечение сотрудников-экспертов транспортных предприятий, имеющих практический опыт реализации требований законодательства для их дальнейшей корректировки с целью улучшения сложившейся ситуации. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Владимир Балановский
Член бюро комиссии РАН по техногенной безопасности, проф. Академии военных наук

Антон Прокопчук
Начальник центра информационных технологий связи и защиты информации ГУ МВД России по г. Москве

Нина Николаева
Помощник члена Совета Федерации

Алексей Авдонов
Генеральный директор "Интерправо Инвест"

Леонид Балановский
Руководитель подразделения ГАУ "МосжилНИИпроект"

Стандарты безопасности объектов инфраструктуры

Объекты инфраструктуры относятся к сложным системам, в состав которых входят взаимосвязанные между собой технические решения и сложные строительные объекты (здания, сооружения с входящими в их состав инженерными сетями и системами поддержания жизнедеятельности, реализации процессов, обеспечения безопасности, энергосбережения, поддержания комфорта и др.). В суровых климатических условиях РФ требуется высочайшая надежность этих систем

С целью обеспечения противостояния угрозам различной природы должен быть применен комплексный подход к объединению всех систем безопасности объектов инфраструктуры в интегрированную систему безопасности (ИСБ). С этой целью должен быть разработан аппаратно-программный комплекс (АПК), позволяющий:

- оперативно реагировать на незаконный пронос/провоз запрещенных веществ (радиоактивных, взрывчатых, отравляющих, биологических, химических, холодного и огнестрельного оружия, боеприпасов);
- интегрировать инженерно-технические средства между собой;
- фиксировать нарушителя с помощью системы видеонаблюдения с выдачей информации на АРМ оператора и для передачи на более высокий уровень;
- определять уровень тревоги;
- выделять нарушителя в многопроходной группе КПП;
- идентифицировать опасные вещества;
- осуществлять мониторинг окружающей среды и систем жизнеобеспечения (систем кондиционирования и вентиляции) на запрещенные вещества.

Такой АПК используется для антитеррористической защищенности объектов (территорий), в соответствии с отраслевыми постановлениями Правительства РФ "Об утверждении требований к антитеррористической защищенности объектов (территорий)".

Основная проблема применения подобных комплексов – их слабая приспособленность к функционированию в составе группы разноотраслевых объектов, объединенных в кластер, или отраслевой территориально разбросанной группы объектов из-за высокой информационной и киберуязвимости.

Необходимость стандартов для критически важных объектов

Согласно постановлению Правительства РФ от 14 августа 2020 г. № 1225 "Об утверждении правил разработки критериев отнесения объектов всех форм собственности к критически важным объектам", объекты инфраструктуры и связанные с ними транспортные системы относятся к критически важным объектам федерального уровня – I категории значимости, объектам, нарушение или прекращение функционирования которых приведет к потере управления экономикой двух и более субъектов РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения двух и более субъектов РФ.

Вопросы обеспечения безопасности и антитеррористической защищенности объектов (включая объекты инфраструктуры) следует решать, начиная с проектирования. Объекты инфраструктуры относятся к высокорисковым критически и стратегически важным объектам, субъектам критической информационной инфраструктуры (КИИ), использующим:

- для управления техническими средствами – геоинформационные системы (ГИС), в том числе системы управления базами данных;
- для работы с людьми (управление персоналом, системы безопасности) – информационные системы персональных данных (ИСПДН).

Наличие этих трех условий (КИИ, ГИС и ИСПДН) предопределяет необходимость разработки стандартов в области обеспечения информационной безопасности и, что особенно важно, их обязательного применения.

Новая парадигма безопасности

Подавляющее число международных, региональных и национальных (включая российские) стандартов в области надежности, безопасности и информационной безопасности, разработанных в XX веке, и часть стандартов, разработанных в первом десятилетии XXI века, были основаны на прежних подходах к вопросам безопасности:

- объект стандартизации – законченный объект (вещь в себе, "черный ящик");
- отсутствие предыстории создания объекта, прослеживаемости его составляющих;
- характеристики объекта – малофакторные, не всегда отражающие свойства объекта в реальных условиях применения;
- вопросы надежности, безопасности, информационной безопасности рассматривались отдельно, независимо друг от друга, без учета их возможной взаимосвязи.

Такие стандарты перестали удовлетворять производителей и потребителей, представителей надзорных и контролирующих органов, страховых и аудиторских компаний.

С первых лет XXI века в мире была принята новая парадигма безопасности, основанная на базовой серии стандартов МЭК 61508 "Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью", Руководстве ИСО/МЭК 51 "Аспекты безопасности. Их применение в стандартах" и серии стандартов ИСО 9000 – ИСО 10000 "Менеджмент качества". Международные стандарты функциональной безопасности систем, связанных с безопасностью, стали быстро развиваться и в первом десятилетии были внедрены во многие области стандартизации. Впервые в мировой практике стандарты функциональной безопасности систем, связанных с безопасностью в строительстве, были созданы в РФ. Это серия ГОСТ Р 53195 [11–15], а также серия ГОСТ 34332 на ее основе, что крайне важно для гарантирования безопасности объектов инфраструктуры.

Комплексный процессный риск-ориентированный подход

Особенность стандартов серий МЭК 61508, ГОСТ Р53195, ГОСТ 34332 состоит в том, что, в отличие от выполнения требований других международных, региональных или национальных стандартов в области безопасности систем, выполнение их требований гарантирует с заданной степенью вероятности достижение и поддержание в период эксплуатации требуемой полноты функциональной безопасности систем и адекватную защиту объектов инфраструктуры.

Разработанные в РФ под руководством В.И. Щербины стандарты серий ГОСТ Р 53195 свыше 10 лет не имели международных и региональных аналогов. На основе их положений первый зарубежный национальный стандарт по одной из СБЗС-систем (VDI 6010, часть 4) только недавно был принят в Германии.

Во втором десятилетии XXI века новая парадигма развивалась на основе стандартов серии МЭК 62443 защиты промышленных коммуникационных сетей, руководств ИСО 26000 "Руководящие указания по социальной ответственности" и МЭК 120 "Аспекты информационной защиты (кибербезопасности) – Руководящие указания по их включению в стандарты". В ней закреплен системный комплексный процессный риск-ориентированный подход с условиями устойчивого развития организаций всех форм собственности, при которых обеспечивается удовлетворение потребностей существующего поколения без риска невозможности удовлетворения потребностей будущих поколений.

Взаимодействие систем и средств информационной защиты и функциональной безопасности

Применительно к объектам инфраструктуры важным является определение различия, взаимосвязи и взаимодействия систем и средств информационной защиты и обеспечения функциональной безопасности.

Системы и средства информационной защиты (ИЗ) ориентированы на противодействие несанкционированному (противоправному) доступу к каналам контроля и управления оборудованием и каналам обмена данными (рис. 1).

Системы и средства функциональной безопасности (ФБ) ориентированы на достижение и поддержание необходимой полноты безопасности электрических, электронных, программируемых электронных систем (включая системы, связанные с безопасностью зданий и сооружений, – СБЗС-системы), а также технических систем и средств ИЗ.

Стандарты на системы информационной защиты и стандарты на системы функциональной безопасности охватывают полный жизненный цикл продукции каждой из систем (рис. 1). В них применены схожие процедуры на стадиях жизненных циклов систем (рис. 2). Их совместное использование приводит к усилению синергетического эффекта. При совместном применении стандартов на ИЗ- и ФБ-системы следует синхронизировать процессы (согласовать скорости соответствующих процессов и интервалы их осуществления).

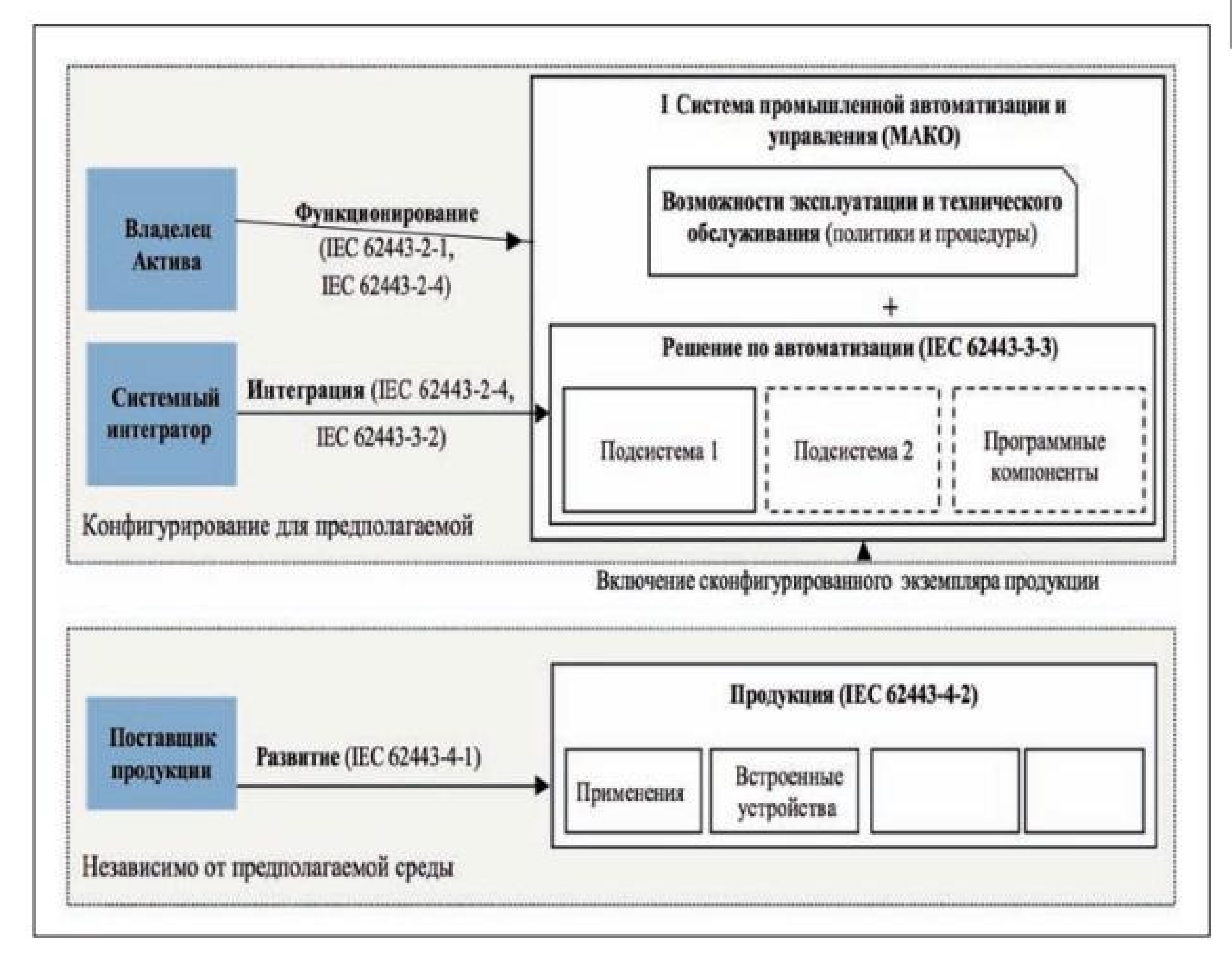


Рис. 1. Стандарты серии МЭК 62443

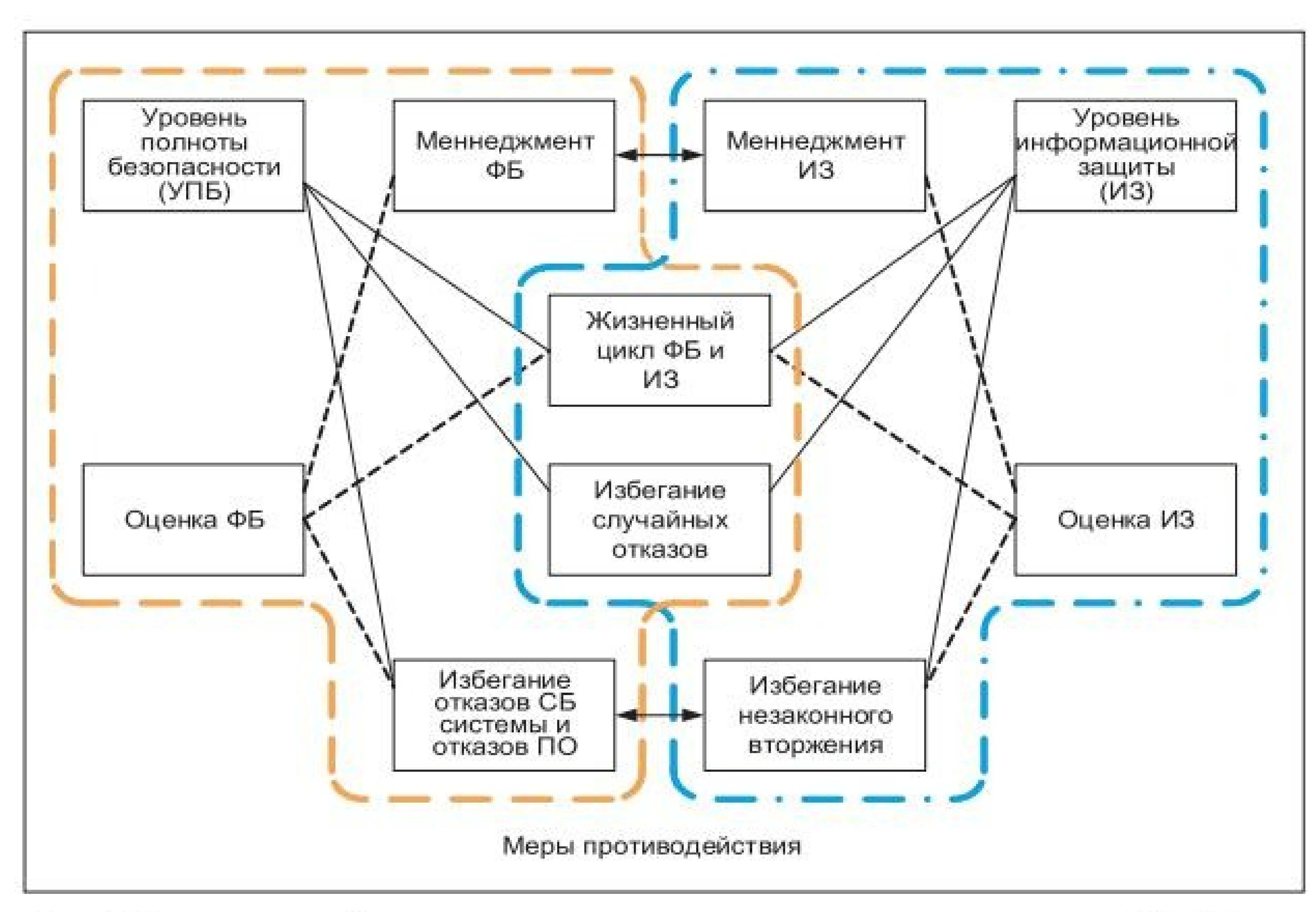


Рис. 2. Схожесть стадий жизненных циклов и процедур в стандартах на системы ИЗ и ФБ

Основные требования к стандартам

В стандартах должен быть применен системный комплексный процессный риск-ориентированный подход, соответствующий условиям обновленной парадигмы обеспечения безопасности и кибербезопасности. Такие стандарты:

- устанавливают требования к средствам, их составляющим, обеспечивающим функциональную безопасность;
- устанавливают требования к функциональной безопасности составляющих объектов инфраструктуры;
- устанавливают требования к информационной защищенности (кибербезопасности) объектов инфраструктуры для обеспечения надежного обмена данными между объектами инфраструктуры;
- определяют различия между требованиями информационной защищенности и функциональной безопасности;
- устанавливают необходимость взаимосвязи на стадиях жизненных циклов объектов инфраструктуры, между специалистами – разработчиками средств и систем, связанных с безопасностью инфраструктуры, со специалистами кибербезопасности;
- содержат рекомендации по построению инфраструктуры и систем.

Стандарты, отвечающие этим требованиям, ориентированы на комплексное обеспечение безопасности и информационной защищенности инфраструктурных систем в целях недопущения неприемлемого риска причинения вреда жизни и здоровью людей, имуществу, окружающей среде. Стандарты учитывают требования к инфраструктурным системам в части обеспечения:

- надежности обмена данными между объектами инфраструктуры для устойчивого и безопасного функционирования их систем;
- информационной безопасности в условиях электромагнитных воздействий природного, техногенного и социогенного происхождения (молниевые разряды, коммутационные помехи, радиочастотные поля, качество сети питания, магнитные поля, переходные и аварийные режимы в энергосистеме, электростатические разряды, геомагнитные токи, промышленные помехи в контурах заземления).

Перспективы применения в производственных системах и системах городского хозяйства

Описанные стандарты посвящены инфраструктурным системам, но могут быть использованы в производственных системах и системах городского хозяйства. Это обеспечит высокую эффективность функционирования объектов инфраструктуры, а применение в обязательном порядке будет способствовать:

- обеспечению функциональной безопасности;
- приобретению конкурентных преимуществ производителями элементов систем, производителями (застройщиками) объектов инфраструктуры, производителями аппаратных средств и программного обеспечения;
- созданию новых рабочих мест на предприятиях – производителях упомянутых систем, застройщиках объектов инфраструктуры;

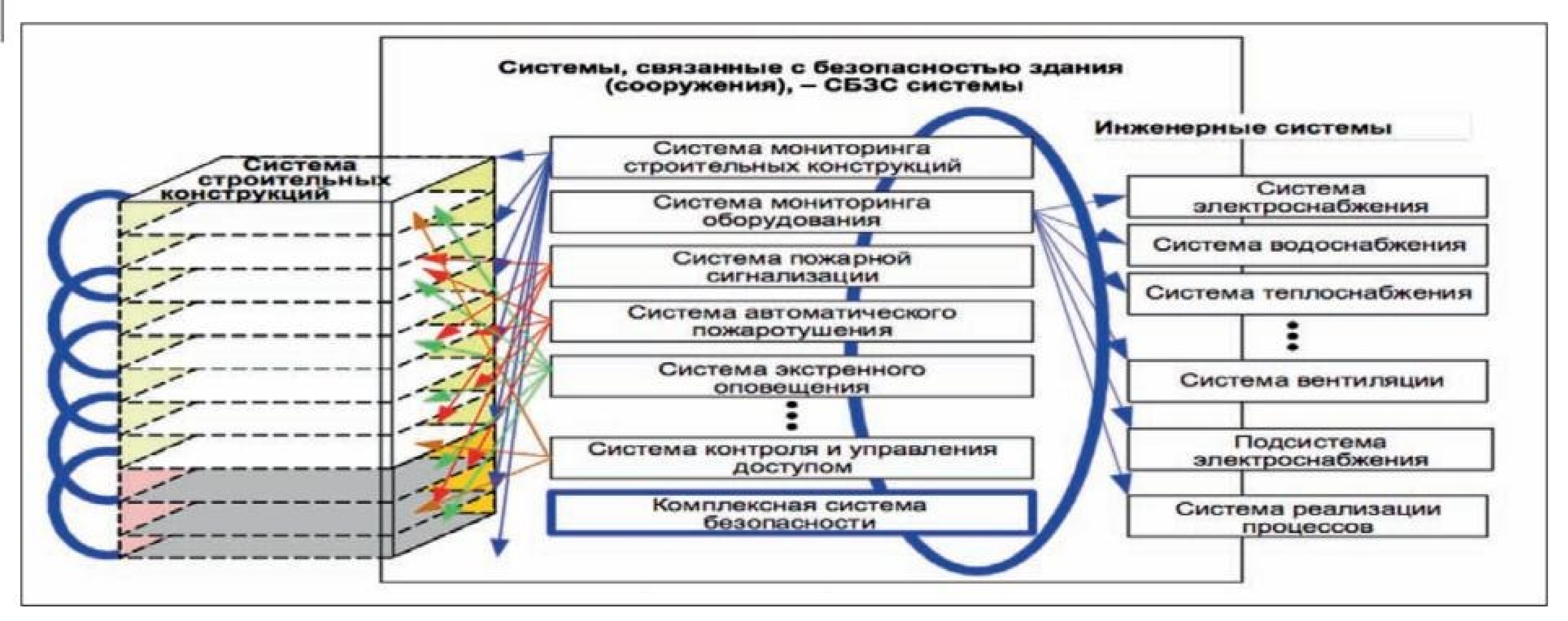


Рис. 3. Модель здания или сооружения как сложной системы

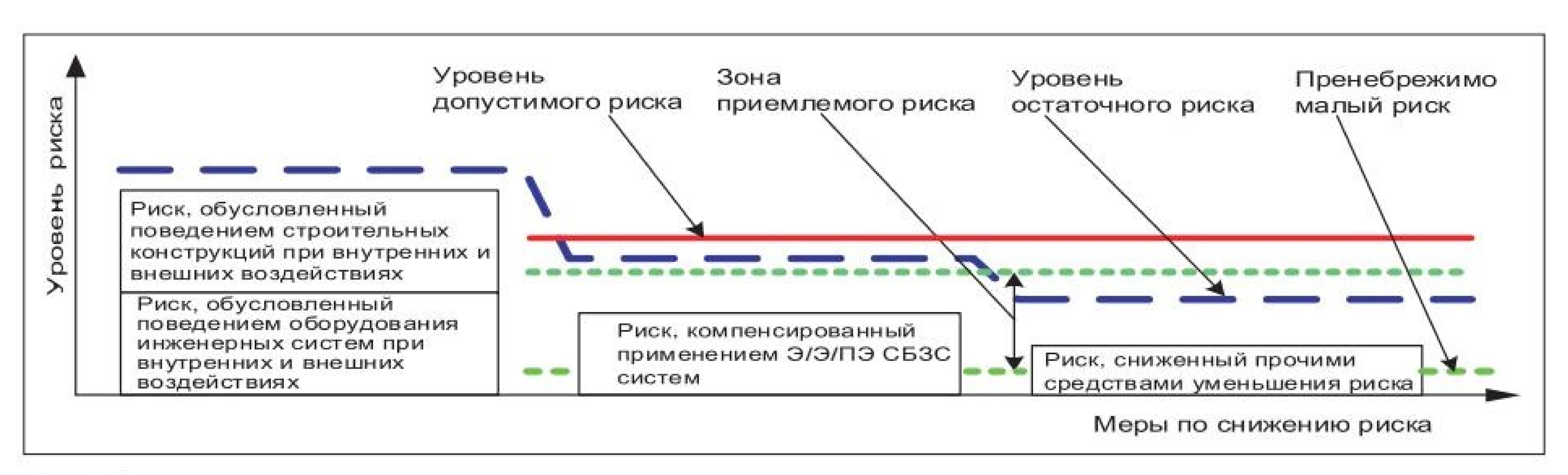


Рис. 4. Снижение риска до приемлемого уровня

- внедрению культуры безопасности и кибербезопасности;
- развитию стандартизации в области других систем;
- более глубокому пониманию регулятивными органами того, что на современном уровне представляют собой системы и инфраструктурные системы, для того чтобы избежать грубых ошибок при подготовке норм правового регулирования;
- интенсификации развития экономики страны.

Информационная защита и функции безопасности как аспекты стандартизации

Объектами стандартизации для обеспечения информационной безопасности являются объекты инфраструктуры, а аспекты стандартизации – это:

- информационная защита данных обмена между объектами инфраструктуры, данных управления и контроля, используемых в технологических процессах;
- обеспечение безопасности систем и их компонентов.

Состав подсистем должен быть научно обоснован по набору функций подсистем, обеспечивающих действия объектовой, региональной системы как единого целого с заданным уровнем безопасности. Объектом инфраструктуры должно быть обеспечено выполнение функций информационной защиты и функций безопасности.

1. Информационная защита:
а) каналов связи приема данных, поступающих от транспортных средств;
б) программируемых систем и средств контроля и управления процессами управления движением, компьютерных систем и средств приема/передачи, обработки и архивирования данных ("ядра" технологических систем управления движением);
в) систем здания или сооружения объекта транспортной системы, осуществляющих внутренний и внешний обмен данными, влияющими на безопасность здания (сооружения), систем жизнеобеспечения, систем, связанных с безопасностью здания и сооружения.
2. Обеспечение безопасности:
а) всех технических средств и систем, используемых для образования каналов связи для обмена данными между объектами инфраструктуры и транспортными средствами;
б) технических средств и систем, входящих в "ядро" технологических систем;
в) технических систем и подсистем, влияющих на безопасность здания или сооружения объекта инфраструктуры транспортной системы.
Здания и сооружения рассматриваются при этом как сложные системы, в состав которых входят системы строительных конструкций и инженерные системы в различных сочетаниях для жизнеобеспечения, реализации процессов, поддержания комфорта, энерго-/ресурсосбережения и обеспечения безопасности. Все эти системы взаимосвязаны, взаимодействуют с внешней и внутренней средами и вместе действуют как единое целое при воздействиях природного, техногенного и антропогенного характера (рис. 3).

Фокус на снижении риска

Для снижения риска применяются системы, связанные с безопасностью зданий и сооружений, а также средства уменьшения риска, которые системами не являются, но их использование приводит к снижению риска (например, инженерные средства безопасности – ограда, ров). Безопасность достигается путем снижения риска, обусловленного внешними и внутренними опасными проектными воздействиями на строительные конструкции и инженерные системы природного, техногенного и антропогенного характера (рис. 4).
Снижение риска осуществляется на всех стадиях и этапах жизненного цикла систем и средств уменьшения риска синхронно со стадиями и этапами жизненного цикла объекта.
Таким образом, комплексный системный процессный риск-ориентированный подход при разработке стандартов в сфере безопасности систем можно расценить как вклад РФ в дальнейшее развитие новой парадигмы безопасности XXI века. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА ЭКСПЕРТА

Что будет после смартфонов?

Сложно представить современный мир без смартфонов и планшетов. Через смартфоны мы читаем новости и общаемся, смотрим и снимаем фото и видео, покупаем товары и оплачиваем услуги, и даже управляем другими устройствами, например устройствами Интернета вещей или умным домом. Фактически смартфон – это окно в мир для современного человека. Но что может прийти ему на смену?



При всех своих удобствах смартфоны имеют и ограничения. Это небольшой экран, который не позволяет полностью погрузиться в цифровой мир. Нужны другие устройства для более полного погружения, которые могли бы использовать уже существующие технологии VR- (виртуальной) и AR- (дополненной) реальности.

Первые шлемы VR появились еще в середине 90-х гг. прошлого века, но до сих пор они не нашли себе массового пользователя, оставаясь лишь игрушками для ИТ-гиков. Основная причина в том, что они не были полноценными устройствами, а лишь дополняли мощные десктопные компьютеры, имели большой вес, давали изображение с недостаточным качеством, а главное – привязывали пользователя к компьютеру проводами, ограничивая его свободу передвижения в виртуальном пространстве. Попытки сделать полностью автономное устройство предпринимали многие компании, например известный проект Google Glasses компании Google, Hololens от Microsoft и многие другие. Но, к сожалению, они так и не вышли как готовые продукты, а остались на уровне прототипов и наборов для разработчиков.

Кроме того, нужно учесть, что сам шлем – лишь небольшая часть экосистемы, которая необходима для полноценного погружения в виртуальный мир. С одной стороны, необходима "железная" составляющая, которая, помимо шлема, состоит из манипуляторов, датчиков положения тела в пространстве и т.д., с другой стороны – множество программ для разных сфер применения, контента, оптимизированного для просмотра в VR, а главное – средства доставки, подобные Apple App Store.

Появление шлемов линейки Oculus Quest компании Oculus, принадлежащей Facebook, которые стали первым автономным продуктом, при этом за достаточно небольшую цену, и стали важной вехой в развитии массового рынка.

Шлемы второго поколения Oculus Quest 2 обладают достаточно интересными возможностями: камеры, установленные на шлеме, позволяют в некоторых случаях обойтись без манипуляторов, используя распознавание движения пальцев рук, что делает взаимодействие с контентом более естественным: пользователь "своими руками" трогает виртуальные объекты, перемещает их в пространстве и т.д.

В этом шлеме есть интересная функция – наложить изображение с камер на виртуальный мир, смешивая реальные и виртуальные объекты в одном пространстве. Пользователь может изменять прозрачность входящего видеопотока или же сделать его черно-белым, оставив виртуальные объекты цветными. Это создает потрясающий эффект, очень похожий на то, как видел мир Фродо из "Властелина колец", когда надевал волшебное кольцо. Кроме того, камеры могут отслеживать положение тела относительно других предметов и стен комнаты и предупреждать пользователя, когда он подходит близко, чтобы избежать ушибов и травм.


www.luminousgroup.co.uk

Для удобного распространения контента Facebook создал собственный магазин VR-приложений, в котором есть достаточно большой выбор от различных разработчиков. В первую очередь это, конечно, игры. Полноценное погружение в игровую реальность дает совершенно незабываемый опыт по сравнению с игрой даже на больших телевизорах. При этом игры могут не только развлекать, но тренировать пользователя. Набирает популярность целое направление специальных фитнес-игр, где в игровой форме пользователь проходит тренировки, от имитации бокса до велогонок.

В связи с последними тенденциями распределенной работы стали очень важны инструменты виртуального офиса. Осенью 2020 г. Facebook представил продукт Infinite Office – виртуальную рабочую среду для корпоративных сотрудников. Офисный работник перемещается по дому в гарнитуре Oculus 2, с помощью которой он редактирует документы, общается с коллегами и просматривает электронную почту. Видео демонстрирует, как работник регулирует прозрачность фона, позволяя смоделированным парящим экранам рабочего стола появляться либо наложенными на фактическое окружение пользователя (имитируя AR), либо в полностью смоделированной обстановке (в данном случае на курорте с пальмами).

Есть целый класс приложений виртуальных мониторов, таких как Immerse, которые могут показывать в виртуальном окружении Quest ваши рабочие мониторы с открытыми окнами программ, запущенных на обычном компьютере. Вы можете работать с вашими обычными рабочими программами прямо из виртуальной реальности, при этом не ограничены размером мониторов и даже их количеством. По субъективным ощущениям пользователей, это напоминает работу с текстом, который выведен на современный телевизор с разрешением Full HD.

Для комфортного взаимодействия не всегда достаточно анализа положения рук через встроенные камеры, поэтому для точных действий в виртуальном пространстве можно использовать манипуляторы, которые идут в наборе. Часто пользователю нужна также обратная связь, особенно при вводе данных, поэтому Facebook и Logitech создали физическую клавиатуру, которую можно подключить к Quest и набирать текст, видя аватар этой клавиатуры в виртуальном пространстве.

Несмотря на достаточно долгую и во многом неудачную историю выхода VR-технологий на массовый рынок, сейчас сложились благоприятные условия для их массового проникновения, особенно в условиях эпидемии и перестройки нашего привычного образа жизни, от развлечений и путешествий до организации работы. На этом фоне очень показательно выглядит отчет PwC, согласно которому в 2019 г. индустрия AR и VR оценивалась в 46 млрд долларов, к 2030 г. она вырастет в 30 раз.

Возможно, мы наблюдаем новый этап развития человеко-машинных интерфейсов, сопоставимый с представлением первого iPhone в 2007 г. ■

Алексей Коржебин
Эксперт редакции журнала "Системы безопасности"





До сих наиболее распространенным видом домофонии являются аналоговые вызывные аудиопанели, лишь иногда прореживаемые моделями с функцией видеосъемки. Однако развитие общества диктует новые условия, стимулируя разработки в области высоких технологий.

Сегодня, в эпоху не отдельно стоящих зданий, а целых жилищных комплексов (ЖК), наделенных самостоятельной инфраструктурой, самым оптимальным вариантом обеспечения безопасности становится IP-видеопанель. Количество вызывных IP-панелей, появляющихся на рынке, неуклонно растет. Данные модели не только способны выполнять свои базовые задачи, но и обладают встроенным видеомодулем, записью видео в архив и возможностью вызова на несколько устройств. В связи с этим наблюдается массовая замена

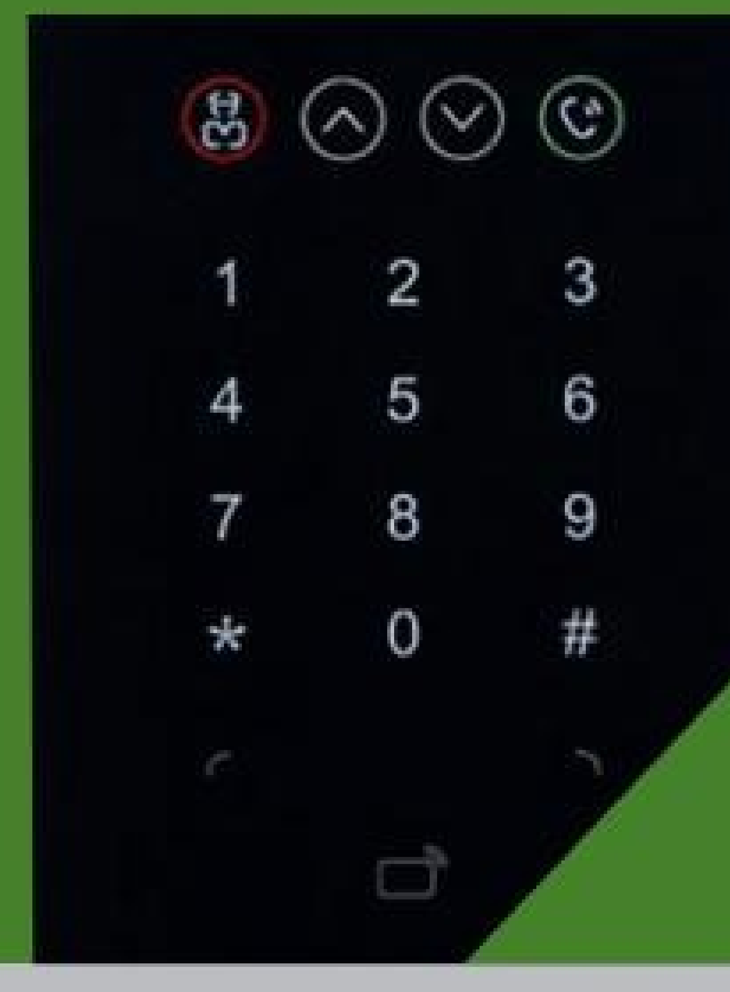
ОБЗОР S&S

старых аналоговых панелей на умную домофонию, более актуальную для таких проектов, как "Безопасный город", благо многие крупнейшие компании, работающие в сфере видеонаблюдения, предоставляют широкий модельный ряд вызывных IP-панелей.



Многоабонентские домофоны с SIP-протоколом





Наиболее же универсальным представляется применение SIP-домофонов со всеми основными преимуществами IP-устройств, в том числе оперативной интеграцией в крупные программные комплексы, что значительно упрощает порядок их внедрения и эксплуатации.

В приведенном обзоре рассмотрены следующие продукты:
- **многоабонентская вызывная IP-панель BAS-IP AA-07B Stainless Steel;**
- **многоабонентский IP-домофон BEWARD DKS15133;**
- **многоабонентская вызывная IP-панель Dahua VTO6521H-D;**
- **многоабонентская вызывная IP-панель Hikvision DS-KD8002-VM**



Обзор предоставлен независимой тестовой лабораторией CCTVLAB

Многоабонентская вызывная IP-панель BAS-IP AA-07B Stainless Steel

Отличительной особенностью AA-07B Stainless Steel является наличие цветного 4,3" TFT-экрана с подсветкой и подогревом, а также IP-камеры высокого разрешения с большими углами обзора. Разрешение камеры, применяемой в панели, составляет 1,3 Мпкс при угле обзора в 80 град. Возможность поворота камеры, заявленная производителем, составляет ±15 град. Видео передается в формате SIP P2P. Встроенное реле дает возможность гибко управлять устройствами входной группы.

Лицевая панель изготовлена из нержавеющий стали марки AISI 304. Толщина панели составляет 3 мм, что делает ее более вандалоустойчивой. Для установки панели используется врезной монтаж. В случае необходимости есть опционная возможность накладного монтажа благодаря использованию BR-AA STAINLESS – кронштейна из нержавеющей стали с козырьком, специально разработанного для вызывных панелей этой серии.

По словам производителя, панель BAS-IP AA-07B Stainless Steel поддерживает технологию UKEY для считывания карт, брелоков и мобильных идентификаторов. Память устройства рассчитана на 20 тыс. ключей.

Температурный режим, заявленный производителем, варьируется от -40 до +65 °C.



Многоабонентский IP-домофон BEWARD DKS15133

Для передачи видео в многоабонентском IP-домофоне BEWARD DKS15133 применяются высокочувствительные сенсоры SONY Exmor с разрешением 1,3 или 2 Мпкс (на выбор). Разрешение основного потока видео в реальном времени составляет 1920x1080 пкс для версии 2 Мпкс и 1280x960 пкс для версии 1,3 Мпкс.

Основным отличием новой модели на своей платформе DKS производитель BEWARD заявляет возможность замены видеомодуля без разборки и демонтажа домофона. При необходимости модуль может быть заменен на модуль с другим разрешением и углом обзора. При заказе производитель предлагает параметры на выбор:

- 1,3 Мкпс, 2,1 мм, 128 град. (по горизонтали);
- 1,3 Мпкс, 2,7 мм, 100 град. (по горизонтали);
- 2 Мпкс, 2,1 мм, 144 град. (по горизонтали);
- 2 Мпкс, 2,8 мм, 112 град. (по горизонтали);
- вариант с пинхол-объективом 1,3 Мпкс, 3,7 мм, 80 град. (по горизонтали).

Опционально доступна возможность вызова через координатно-матричные аналоговые сети до 600 абонентов.

IP-домофон может работать через IP-АТС или связываться с другим SIP-устройством напрямую. DKS15133 дает возможность принимать вызов и открывать дверь (тональный набор DTMF) при переадресации на обычный сотовый или городской телефон. На каждого абонента заявлена возможность настроить до пяти направлений вызова. Поддерживается 4-значный номер абонента до 9999, что позволяет применять IP-домофон в гостиницах либо в зданиях с большой этажностью. Наличие RFID-считывателя MIFARE ID помогает организовать проход в подъезд по беспроводным меткам.

IP-домофон BEWARD DKS15133 оснащен аппаратной обработкой аудиосигнала и системой эхоподавления, которые, по словам производителя, позволяют получить четкий, хорошо распознаваемый звук.

Металлический антивандальный корпус IP-домофона не даст злоумышленникам вывести его из строя, а встроенный концевой выключатель



вскрытия сообщит о попытке снятия с места установки. Уровень защиты от пыли и влаги соответствует классу IP66. Для врезной установки предусмотрен кронштейн, позволяющий закрепить устройство на стенах из бетона, газобетона, кирпича, ПГП.

Производителем заявлен температурный режим от -50 до +60 °C.

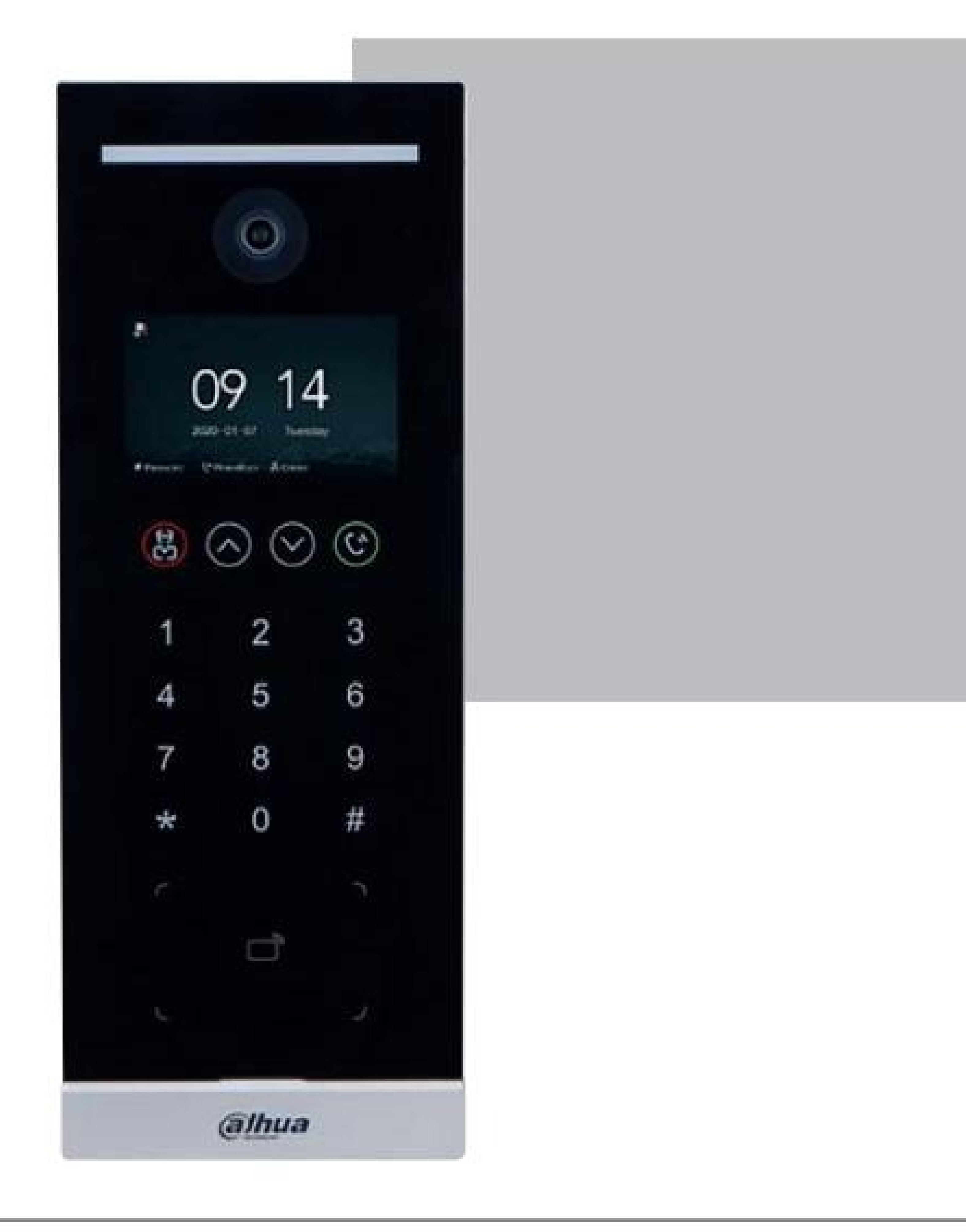
Многоабонентская вызывная IP-панель Dahua VTO6521H-D

Устройство обладает 4,3" IPS-дисплеем с разрешением экрана 800×480 пкс. Согласно параметрам, заявленным производителем, основной видеопоток имеет разрешение 720p при частоте 25 кадр/с, тогда как разрешение дополнительного потока составляет 1080p при частоте 30 кадр/с. Видеокамера обладает следующими параметрами: 1/2,7" CMOS, 2 Мпкс, высокое разрешение, низкая освещенность, белый свет, ИК-подсветка. Угол обзора составляет 113,79 град. по горизонтали, 61,5 град. по вертикали и 134,45 град. по диагонали. Фокусное расстояние – 2,8 мм. В устройстве обеспечена поддержка SIP-сервера, который управляет домофонами (до 200 единиц).

Корпус вызывной панели изготовлен из пластика с применением ударопрочной технической термопластической смолы (АБС-пластик). На корпусе размещаются сенсорные кнопки с степенью защиты IP65. Для установки панели применяется как накладной, так и врезной монтаж. Для врезной установки используется металлический короб VTM130 от производителя.

В устройстве имеются разные режимы открытия: с помощью пароля, IC-карты и дистанционно. Согласно утверждению производителя, осуществляется поддержка 20 тыс. пользователей и 10 тыс. карт, а также полнодуплексной связи. Управление и голосовая связь доступны через специальное приложение. В наличии поддержка тревоги принуждения, тампера (контакт несанкционированного вскрытия) кражи и сигнала о превышении времени ожидания для датчика двери.

Температурный режим, заявленный производителем, от -30 до +60 °C.



Многоабонентская вызывная IP-панель Hikvision DS-KD8002-VM

Многоабонентская вызывная панель построена на базе ОС Linux. Вся информация отображается на 3,5" сенсорном TFT-дисплее с максимальным разрешением 480x320 пкс (подсветка включается посредством ИК-датчика автоматически). Модель оборудована IP-видеокамерой с CMOS-матрицей и максимальным разрешением 1280x720 пкс, скорость трансляции потока – 25 кадр/с в реальном времени. Угол обзора составляет 120 град. В условиях недостаточной освещенности и полной темноте превосходную видимость сцены обеспечивает встроенная LED-подсветка. Поддерживаются сетевые протоколы TCP/IP, SNMP, SIP, RTSP. При подключении встроенной IP-камеры панели DS-KD8002-VM к системе TRASSIR по RTSP-протоколу видео с нее, синхронизированное со звуком, может быть записано на сервер TRASSIR или в облако TRASSIR Cloud, что требует дополнительного приобретения соответствующей лицензии. Система домофонии на базе оборудования Hikvision также допускает подключение до 16 обычных IP-камер видеонаблюдения.

Корпус, выполненный из алюминиевого сплава, соответствует стандарту защиты от попадания внутрь влаги и пыли IP65. Для осуществления прохода можно вызвать абонента, воспользовавшись блоком механических клавиш, или прибегнуть к помощи встроенного считывателя IC-карт. Имеется кнопка вызова консьержа. Для организации двусторонней аудиосвязи с домофонными IP-мониторами системы и пультом консьержа модель снабжена встроенными динамиками и микрофоном с шумо- и эхоподавлением. В числе интерфейсов: сетевой разъем RJ-45, тревожные входы/выходы (8/4), RS-485, Wiegand, USB2.0, порт подключения БП 12 В. Максимальное энергопотребление модели составляет 12 Вт. Имеются датчик двери и тампер, выручающий в ситуации несанкционированного демонтажа. Физические размеры – 418x145x61 мм. Бокс для врезного монтажа в комплекте.



Температурный режим, заявленный производителем, варьируется от -40 до +70 °C.

Новые грани домофонии

Возможности применения SIP-протокола в многоабонентских вызывных панелях достаточно эффективны и уже оценены по достоинству. SIP-протокол дает возможность внедрить практически любое совместимое устройство в любое место системы.

Домофонные системы, совместимые с SIP-протоколом, обладают огромными возможностями расширяемости и масштабирования. Благодаря этому на оборудованных объектах возможна реализация различных комплексных решений. Применение IP-устройств в жилых кварталах или крупных офисных центрах позволяет создать развитую инфраструктуру для контроля и наблюдения, доступную как монтажным организациям, так и жильцам.

Нельзя забывать и тот факт, что развитие данных устройств стимулирует провайдеров цифровых услуг на создание все новых и новых сервисов для жильцов, направленных на облегчение их жизни. Уже сейчас разработаны новые программы, позволяющие управлять домофоном с помощью не только мобильного телефона, но и телевизионного пульта. Активно внедряется программное обеспечение, направленное на интеграцию домофонных сетей с социальными и экстренными службами (скорая помощь, полиция, МЧС, пожарные и т.д.). Таким образом, грани применения классических принципов домофонии существенно расширяются и открывают дорогу новым стадиям развития возможностей СКУД. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Охранные извещатели в центре внимания



Заметным событием весны стала выставка Securika Moscow 2021. В рамках программной части выставки прослеживался повышенный интерес посетителей к семинарам и конференциям, посвященным новым сводам правил МЧС в области проектирования систем пожарной автоматики. Наиболее детальное обсуждение вопросов и разъяснение к ним было сконцентрировано в отношении СП 484.1311500.2020, о котором мы неоднократно упоминали в предыдущих материалах. Поэтому сегодня хотелось бы уделить должное внимание результатам юбилейного 25-го конкурса "Лучший инновационный продукт" именно в части охранной сигнализации, которой в последнее время уделялось меньше внимания.



Фото с церемонии награждения победителей конкурса "Лучший инновационный продукт"

Как отметили на церемонии вручения наград представители конкурсного жюри, в этом году представленные материалы показались им "самыми инновационными", в номинации "Охранная сигнализация" при этом победили сразу три продукта.

Первый – извещатель охранный объемный совмещенный радиоканальный для защиты музейных экспонатов и витрин. Он позволяет обнаруживать как разрушение остекленной поверхности музейной витрины, так и проникновение руки в контролируемый объем витрины. Очень плотная зона обнаружения позволяет фиксировать перемещение руки на 30 см. Кроме того, контролируется наклон, перемещение витрины и отрыв извещателя от ее поверхности. Подобного комплексного и малогабаритного (35×66×72 мм) решения еще не было представлено на рынке. Удобство монтажа, достигаемое за счет передачи тревожных сигналов по радиоканалу, также дает дополнительные преимущества этому изделию. Данное изделие, безусловно, найдет своего потребителя среди множества федеральных и региональных музеев в нашей стране, особенно в свете резонансного происшествия с картиной А. Куинджи.

Второй победитель конкурса – еще один радиоканальный извещатель для защиты музейных экспонатов. Точечный тензометрический датчик, работающий по "принципу безмена", контролирует подвес картины и реагирует на минимальные изменения ее веса. Это первое подобное решение на рынке. Оно лишено недостатков широко применяемых для защиты экспонатов герконовых датчиков, датчиков движения или перемещения. Оптико-электронные извещатели трудно разместить в выставочных залах так, чтобы они не выдавали ложные срабатывания при большом количестве посетителей. Если злоумышленники не передвигают картину, а, например, вырезают холст из рамы, то и геркон, и датчики наклона и перемещения могут не сработать. При этом тензометрический извещатель, реагирующий только на изменение веса, с намного меньшей вероятностью будет выдавать ложные срабатывания, притупляющие бдительность смотрителей, и при этом сработает при похищении холста из рамы. В извещателе также применен радиоканал, позволяющий передавать сигналы даже в условиях старых зданий со стенами большой толщины.

Третьим победителем стал извещатель адресный охранный поверхностный звуковой для контроля и защиты остекленных поверхностей. Известно, что кроме обеспечения функции обнаружения разрушения стекла перед современными акустическими извещателями встает дополнительная важная задача – противостояние саботажу, то есть контроль появления посторонних предметов, закрывающих отверстие в корпусе, через которое акустические сигналы разрушения стекла попадают на встроенный микрофон. Антимаскирование традиционно реализовывалось двумя способами. Первый из них заключался в использовании пьезоэлектрического излучателя, периодически генерирующего звуковой сигнал в слышимом диапазоне. При наличии постороннего предмета около микрофонного отверстия акустическая картина менялась, что интерпретировалось извещателем как факт саботажа. Еще одним плюсом такой реализации был дополнительный контроль исправности микрофона во время эксплуатации. Главным же недостатком являлась "слышимость" тестового сигнала внутри помещения, который в ряде случаев создавал дискомфорт для человека, находящегося долгое время в непосредственной близости от установленного изделия. По этой причине максимальная мощность тестового сигнала была сильно ограничена. Альтернативным вариантом реализации антимаскирования было использование ИК-пироэлектрика, который позволял уверенно обнаруживать появление посторонних предметов рядом с извещателем, не вызывая дискомфорта у персонала защищаемого объекта, но при этом терялся контроль работоспособности микрофона.

В представленном на конкурс извещателе был применен новый подход к реализации функционала антимаскирования, основанный на инновационном развитии первого из вышеописанных методов. Для формирования тестового сигнала в нем используется пьезоэлектрический излучатель, но работающий в ультразвуковом диапазоне частот, не воспринимаемом человеком на слух. За счет этого появилась возможность снять ограничения по мощности тестового сигнала. Современный МЭМС-микрофон, примененный в качестве чувствительного элемента, "слышит" одновременно звуковой и ультразвуковой диапазоны. Таким образом, представленное решение обладает всеми достоинствами аналогичных извещателей, но лишено их недостатков. Дополнительным плюсом является также значительное увеличение угла зоны обнаружения.

Отрадно, что все три извещателя-победителя были разработаны российскими компаниями, что еще раз продемонстрировало огромный потенциал отечественных разработок.■

Максим Горяченков
Редактор раздела "ОПС, пожарная безопасность", руководитель отдела технической поддержки ЗАО НВП "Болид"



Реализация механизма "регуляторной гильотины": взгляд глазами ритейла

В 2019 г. был запущен новый этап реформы системы государственного контроля и надзора, который связан с механизмом "регуляторной гильотины". Ее целью является комплексное обновление обязательных требований, принятых ранее середины 2010 г., с одновременным проведением анализа фактических положительных (отрицательных) последствий утверждения нормативных правовых актов, а также достижения заявленных целей регулирования. В данной статье я хочу проанализировать, каким образом мероприятия, проводимые в рамках указанной реформы, в том числе по вопросам пожарной безопасности, отразились на бизнесе и ритейле в частности

Виталий Данченков
Руководитель направления пожарной безопасности компании X5 Retail Group

Нововведения призваны отсечь требования, содержащиеся в нормативных правовых актах, которые в настоящее время утратили свою актуальность, не проходили процедуру экономической оценки их эффективности и существенно влияют либо затрудняют ведение предпринимательской деятельности.

От 100 нормативных актов к 7 новым законам

Оптимизация обязательных требований в области пожарной безопасности не была такой продуктивной и показательной, как, например, в области санитарных требований. Так, например, при выполнении всех требований санитарных норм для медицинского учреждения требовалось построить здание площадью 11 тыс. кв. м. После "регуляторной гильотины" медицинское учреждение, рассчитанное на такое же количество пациентов и имеющее аналогичный набор услуг, уже может иметь площадь в 8 тыс. кв. м. Конечно, это существенные сокращения затрат для экономики, которые можно использовать на ее развитие.

В пожарной безопасности сложно привести такие же замечательные примеры. А причина такого положения в том, что МЧС России реформу обязательных требований провело еще в 2009 г., основой которой стал ФЗ-123 "Технический регламент о требованиях пожарной безопасности", легализующий "гибкую" систему противопожарного нормирования. Вместе с тем в рамках текущей "регуляторной гильотины" МЧС России провело существенную работу, пересмотрев более 100 нормативных актов в области пожарного надзора, вместо которых созданы семь новых федеральных законов.

ФЗ-247 "Об обязательных требованиях"

Главным достижением "регуляторной гильотины" является принятие Федерального закона от 31 июля 2020 г. № 247-ФЗ "Об обязательных требованиях". Этот законодательный акт – основа всей регуляторной реформы. Его главные принципы: законность, обоснованность, правовая определенность и системность, открытость, предсказуемость и исполнимость обязательных требований.

Необходимым условием установления обязательных требований является наличие риска причинения вреда. Если несоблюдение какого-либо требования не приносит на протяжении большого количества лет никакого вреда, значит, это требование не должно быть обязательным. Их будут пересматривать один раз в шесть лет.

Все обязательные требования должны быть исполнимыми. При их формировании необходимо учитывать затраты лиц, в отношении которых они устанавливаются, на их исполнение. Расходы должны быть соразмерны рискам, предотвращаемым этими требованиями, при обычных условиях гражданского оборота.

Отдельно хотелось бы остановиться на обоснованности обязательных требований. При работе в экспертной группе очень часто на наши предложения приходили ответы надзорных органов: нецелесообразно, так как требование влияет на безопасность людей, пожарных и т.д.. При этом не давалось каких-то веских аргументов. Просто так считалось и считается на протяжении десятков лет. Теперь же на надзор возложено бремя доказывания необходимости соблюдения обязательного требования. Главное при реализации ФЗ-247 – установить системность влияния обязательных требований на реальную жизнь и оценивать эффективность этих мероприятий не каким-то эфемерным образом, а на основании наблюдений, статистических данных, расчетов и т.д.

ФЗ-248 "О государственном контроле (надзоре) и муниципальном контроле в РФ"

Важной частью механизма "регуляторной гильотины" стал Федеральный закон от 31 июля 2020 г. № 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в РФ". Данный законодательный акт закрепляет и конкретизирует уже апробированную на практике риск-ориентированную модель надзора.

Ключевое отличие по линии пожарного надзора нового закона от ФЗ № 294 "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" отражено в ст. 16. Определено, что объектами





государственного надзора наряду с деятельностью граждан и организаций являются здания, помещения, сооружения, линейные объекты, территории, включая водные, земельные и лесные участки, оборудование, устройства, предметы, материалы, транспортные средства и другие объекты, которыми граждане и организации владеют и (или) пользуются и к которым предъявляются обязательные требования.

Таким образом, при планировании проверок в 2022 г. ГПН будет применяться принцип "один объект (здание) – одна проверка". Безусловно, количество проверок в отношении объектов нашей компании увеличится.

Думаю, что основные вопросы по планированию проверок появятся в следующем году, поэтому МЧС России надо организовать среди субъектов экономики соответствующую разъяснительную работу. Также МЧС России должно довести до бизнеса принципы и подходы, которые будут реализовываться при проверках помещений, арендуемых в зданиях различного назначения. Даже сегодня этот аспект надзорной деятельности не совсем понятен, и ряд наших магазинов планово проверяют как в составе торгового центра (при проверке собственника здания), так и как самостоятельный объект надзора. Причем это происходит в течение одного календарного года.

ФЗ-123 "Технический регламент о требованиях пожарной безопасности" и нормативные документы по пожарной безопасности

В рамках реформы были переработаны положения ФЗ-123, которые прошли общественные обсуждения и будут приняты в 2021 г. Какое из них хочется выделить?

Компания X5 Retail Group первая в российском ритейле внедрила в практику использование стандарта организации по противопожарной защите однотипных объектов (гипермаркеты, супермаркеты, распределительные центры). Несмотря на утверждение данных документов в МЧС России и регистрацию их в качестве нормативных документов по пожарной безопасности, часто инспектора на местах не учитывали их положения при проверках наших объектов. Приходилось получать дополнительные разъяснения, обжаловать решения. В проекте изменений в закон стандарты организаций включены в перечень федеральных нормативных документов по пожарной безопасности наряду со сводами правил, что существенно повысит их статус и расширит для бизнеса возможность применения.

Несмотря на то что "регуляторная гильотина" направлена на пересмотр обязательных требований, МЧС России проводится большая работа по оптимизации норм добровольного применения, изложенных в сводах правил. Актуализация нормативных документов по пожарной безопасности направлена в том числе на исключение необходимости разработки специальных технических условий по обеспечению пожарной безопасности объектов защиты. В настоящее время приказом МЧС России от 15.01.2020 г. № 14 утвержден свод правил "Многофункциональные здания. Требования пожарной безопасности", устанавливающий требования к объектам, состоящим из частей различных классов функциональной пожарной опасности, а также с наличием многосветных пространств. Внедрение свода правил позволяет бизнесу исключить разработку специальных технических условий при проектировании многофункциональных торговых центров и сэкономить время, которое затрачивается на сложные согласовательные процедуры.

В полном объеме переработан свод правил СП 1.13130 "Системы противопожарной защиты. Эвакуационные пути и выходы". Не без нашего участия в документ наконец-то вводится понятие "основной эвакуационный проход в торговом зале". То есть требования к основным эвакуационным проходам у нас были всегда, а вот самого понятия до выхода этой редакции СП не существовало. Поэтому, согласно статистике, в 90% документов ГНП по результатам проведенных проверок на объектах компании фигурировало нарушение по ширине проходов.

О "добровольности" применения нормативных документов по пожарной безопасности

"Гибкая" система противопожарного нормирования основана на обязательном соблюдении требований нормативно-правовых актов и добровольном применении нормативных документов. И такая "гибкость" тоже имеет свои изъяны и требует изменений.

У нас достаточно много магазинов, которые размещаются в зданиях торговых центров. При наличии незначительных отступлений от требований сводов правил (например, по путям эвакуации в торговом зале) все нормы добровольного применения автоматически становятся обязательными, ведь практически невозможно просчитать пожарные риски для всего здания, так как оно уже введено в эксплуатацию и в нем размещается множество других арендаторов.

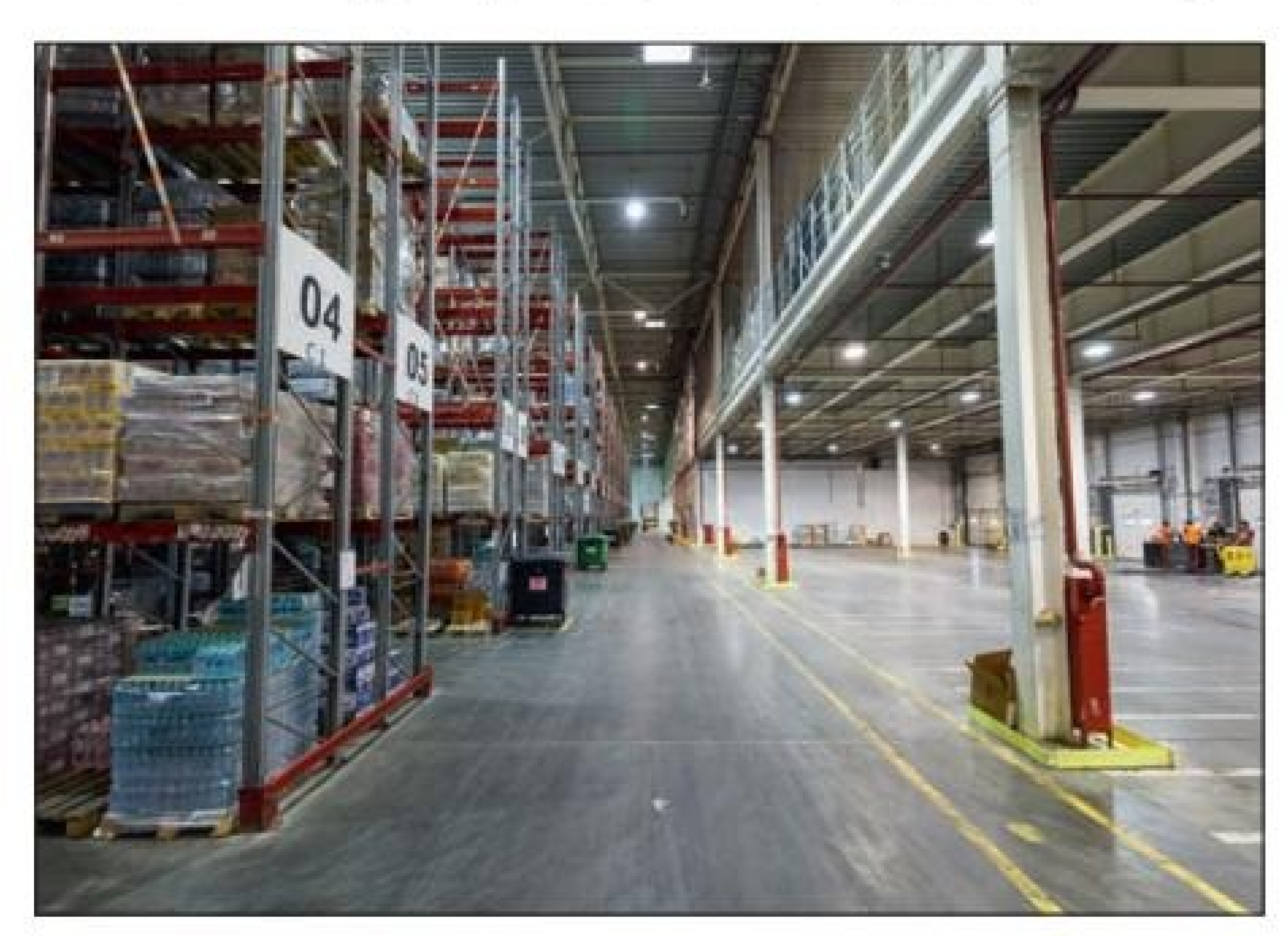
Или другой пример. Если расстояние между насосными агрегатами не соответствует требованиям свода правил, становится ли от этого система пожаротушения менее эффективной? И может ли в таком случае система учитываться при проведении расчетов пожарного риска?

По моему мнению, при актуализации требований нормативных документов МЧС России целесообразно применять принципы, описанные выше в ФЗ-247 (хотя эти требования "условно" добровольные). Особенно это касается наиболее затратных мероприятий. Рассмотрим на примере внутреннего противопожарного водопровода. В монтаж, содержание и обслуживание внутреннего противопожарного водопровода субъекты экономики ежегодно вкладывают значительные средства. И если взять эти затраты в рамках всего государства, получится гигантская сумма. А кто провел анализ, сколько было за год потушено пожаров внутренним противопожарным водопроводом? Какой ущерб предотвращен посредством противопожарного водопровода и как он соизмеряется с размером вкладываемых средств? На объектах какой функциональной пожарной опасности применялся ВПВ? Какие риски существуют при его отсутствии? Я не утверждаю, что от ВПВ надо полностью отказаться. В складских зданиях он необходим, но каждое требование надо пересматривать на основании оценки эффективности и риска возможных вероятностей ущерба. Необходимо создать систему в МЧС России, которая сможет оценить влияние того или иного мероприятия на реальную ситуацию с пожарной безопасностью.

Новые Правила противопожарного режима в РФ

С начала 2021 г. вступили в силу новые Правила противопожарного режима в РФ, утвержденные постановлением Правительства РФ от 16 сентября 2020 г. № 1479.

С участием экспертного сообщества и других заинтересованных лиц положения правил изме-







нялась на протяжении двух последних лет, и многие требования были оптимизированы. В новой редакции исключено 20% старых требований, которые носили номинальный характер, не соответствовали современным реалиям или не оказывали влияние на пожарную безопасность объектов.

Для меня показательным примером являются изменения в Правилах по расстоянию от хранимых товаров до светильников в складских помещениях. В нашей компании уже на протяжении как минимум 10 лет применяются только светодиодные светильники, которые не оказывают теплового воздействия на близко расположенные вещества и материалы. Учитывая, что существующая бизнес-модель магазина направлена на увеличение площади торгового зала (для расширения ассортимента продаваемых товаров) и, соответственно, уменьшение складских помещений, очень сложно обеспечить 0,5 м от товаров до светильников. И это при том, что риски возникновения пожара отсутствуют. Но ППР не разграничивали виды светильников, поэтому в каждом третьем административном протоколе ГПН фигурировало данное нарушение. Еще в начале реформы от X5 Retail Group исходило предложение по пересмотру данного требования, и оно, наконец, нашло свое отражение в п. 288 новых Правил. Теперь требование касается только светильников с лампами накаливания, что абсолютно обоснованно.

В новых Правилах есть еще несколько нововведений, в том числе по ведению единого журнала по эксплуатации противопожарной защиты, но без практики применения оценивать их преждевременно.

Не могу не отметить противоречивый момент нового документа. В 2020 г. на рассмотрение экспертной группы поступал проект Правил, который содержал п. 104, запрещающий хранение горючих товаров или негорючих товаров в горючей упаковке в помещениях, не имеющих открывающихся оконных проемов или систем дымоудаления с механическим приводом, за исключением случаев, установленных нормативными правовыми актами или нормативными документами по пожарной безопасности. В действующей редакции из данного пункта исключена часть последнего предложения – "за исключением случаев, установленных нормативными правовыми актами или нормативными документами по пожарной безопасности". Таким образом, с 1 января 2021 г. почти 18 тыс. объектов нашей компании перестали соответствовать требованиям Правил противопожарного режима в РФ, но при этом продолжают соответствовать нормативным документам по пожарной безопасности (СП 7.13130). Выполнение данных требований ППР РФ будет связано с многомиллионными затратами, а во многих случаях они в принципе невыполнимы без реконструкции магазинов. На состоявшемся в начале 2021 г. совещании представители ДНДиПР МЧС России признали данное противоречие и пообещали внести изменения при ближайшей корректировке Правил.

Гармонизация строительных и противопожарных норм

В настоящее время минимальные требования пожарной безопасности к зданиям и сооружениям устанавливаются двумя федеральными законами – это Технический регламент о безопасности зданий и сооружений (Федеральный закон от 30 декабря 2009 г. № 384-ФЗ) и Технический регламент о требованиях пожарной безопасности (Федеральный закон от 22 июля 2008 г. № 123-ФЗ). При этом указанные требования противоречат и взаимно исключают друг друга.

Все экспертное сообщество полагало, что в рамках "регуляторной гильотины" эти противоречия будут исключены. Но 4 июля 2020 г. вышло постановление Правительства РФ № 985 "Об утверждении перечня национальных стандартов и сводов правил (частей таких стандартов и сводов правил), в результате применения которых на обязательной основе обеспечивается соблюдение требований Федерального закона "Технический регламент о безопасности зданий и сооружений".

Данный документ меня разочаровал. Нельзя оспорить, что количество обязательных требований по вопросам пожарной безопасности в строительных нормативных документах сокращено и некоторые изменения нам действительно облегчат жизнь. Так, у нас в компании еще в 2017 г. разработан стандарт организации (СТО) с требованиями пожарной безопасности для распределительных центров (в том числе с наличием охлаждаемых помещений). СТО соответствовал законодательству о стандартизации и был зарегистрирован МЧС России как нормативный документ по пожарной безопасности.

Целями его создания были оптимизация противопожарной защиты в рамках действующего законодательства и отказ от разработки специальных технических условий на каждый объект компании. Но требования строительных норм не позволяли нам использовать СТО, так как площадь охлаждаемых помещений была ограничена обязательными требованиями, которые не соответствовали нашей операционной модели. Любые отступления от обязательных требований согласно ФЗ-384 могли быть обоснованы только разработкой специальных технических условий, с обязательным согласованием в МЧС России и Минстрое, что нам и приходилось выполнять.

Ограничения по охлаждаемым камерам постановлением Правительства РФ № 985 выведены из разряда обязательных, что позволяет реализовать СТО в полном объеме и сокращает расходы и время на проектирование распределительных центров.

Но в целом проблема гармонизации не решена, и в перечне обязательных положений строительных норм фигурируют требования по пожарной безопасности. В частности, обязательный характер исполнения продолжают иметь положения СП 56.13330.2011 "Производственные здания", определяющие требования к площади пожарных отсеков, степени стойкости зданий и т.д. В случае отступления от них необходимо разрабатывать специальные технические условия со всеми обременениями. В пожарных нормах аналогичные требования имеют статус добровольного применения, от которых можно отступать при подтверждении безопасности людей расчетами пожарных рисков.

Аналогичная ситуация со сводом правил СП 118.13330.2012 "Общественные здания и сооружения", где практически все требования по эвакуации людей отнесли в разряд обязательных. Налицо прямые противоречия двух систем нормирования.

Следует отметить, что МЧС России продолжает работу по гармонизации нормативных документов, и будем надеяться, что она завершится в текущем году.

Движение в нужном направлении

В заключение отмечу, что в целом реформа определила правильное направление развития как нормативной базы, так и надзорной деятельности в стране. Бизнес-сообщество принимает активное участие в этих процессах и надеется на установление баланса между интересами бизнеса и государства. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Статья опубликована в каталоге "Пожарная безопасность", 2021 г.

Распознавание лиц – новое качество ИСО "Орион"!

Тема распознавания лиц в контексте различных задач находится на пике популярности в области видеонаблюдения и контроля и управления доступом. Нередко целые номера специализированных журналов посвящают проблеме распознавания лиц и идентификации личности, ее обсуждают на форумах и онлайн-конференциях. Как правило, под распознаванием лиц понимается визуальное обнаружение лица и последующая процедура персональной идентификации по заранее сформированной базе данных. В популярной интегрированной системе охраны "Орион" распознавание лиц получило свою реализацию с помощью двух технологий: аппаратной и программной. При этом для каждой обозначились свои задачи, решаемые при идентификации лиц персонала объектов

В оборудование контроля доступа ИСО "Орион" добавилось сразу два биометрических контроллера, обладающих нужным функционалом для идентификации лиц: "С2000-BIOAccess-SF10" (рис. 1) и "С2000-BIOAccess-SF10T" (рис. 2).

Характеристики контроллеров распознавания лиц

Оба контроллера позволяют работать с базой до 10 000 шаблонов лиц, хранить события в энергонезависимом буфере емкостью до 100 000 записей, отображать информацию на 7" цветном сенсорном TFT-дисплее, имеют встроенную сдвоенную видеокамеру с разрешением 2 Мпкс, выходы управления замком (турникетом) и предназначены для установки в помещениях без отрицательных температур. Они поддерживают расстояние идентификации от 0,5 до 3 м и скорость идентификации менее 1 с, это дает возможность применять их как на турникетах проходной, так и в настенном варианте при монтаже у входных дверей в отдельные помещения здания.

"С2000-BIOAccess-SF10T" отличается наличием встроенного тепловизора, что позволяет на расстоянии 25–50 см измерить температуру тела. Дополнительно в этом контроллере заложены алгоритмы определения наличия на лице медицинской маски, корректности ее ношения, а также считыватели дополнительных идентификационных признаков: отпечатка пальца и Proximity-карт.

Работа в составе ИСО "Орион"

Контроллеры могут работать как автономно, так и в составе ИСО "Орион". База шаблонов биометрических идентификаторов со списком прав доступа для каждого шаблона хранится в контроллере, в собственной энергонезависимой памяти. Обновление базы идентификаторов производится из программных модулей АРМ "Орион-Про".

При использовании биометрических контроллеров доступен весь основной функционал подсистемы контроля доступа ИСО "Орион": ведение журнала событий (успешная идентификация, проход, доступ запрещен, дверь открыта, дверь закрыта, дверь взломана и т.д.), формирование различных отчетов, организация учета рабочего времени.

Push-протокол и модуль BAServer

Для взаимодействия программного обеспечения АРМ "Орион Про" с "С2000-BIOAccess-SF10" и "С2000-BIOAccess-SF10T" используется проприетарный протокол Push, который интегрирован в прошивку контроллера.

Связь со всеми биометрическими контроллерами осуществляется через отдельный входящий в состав АРМ "Орион Про" модуль BAServer. Сами контроллеры взаимодействуют с модулем BAServer как по локальной сети, так и через Интернет. Пример организации взаимодействия программных модулей АРМ "Орион Про" и биометрических контроллеров представлен на рис. 3.



Рис. 1. Биометрический контроллер "С2000-BIOAccess-SF10"



Рис. 2. Биометрический контроллер "С2000-BIOAccess-SF10T"

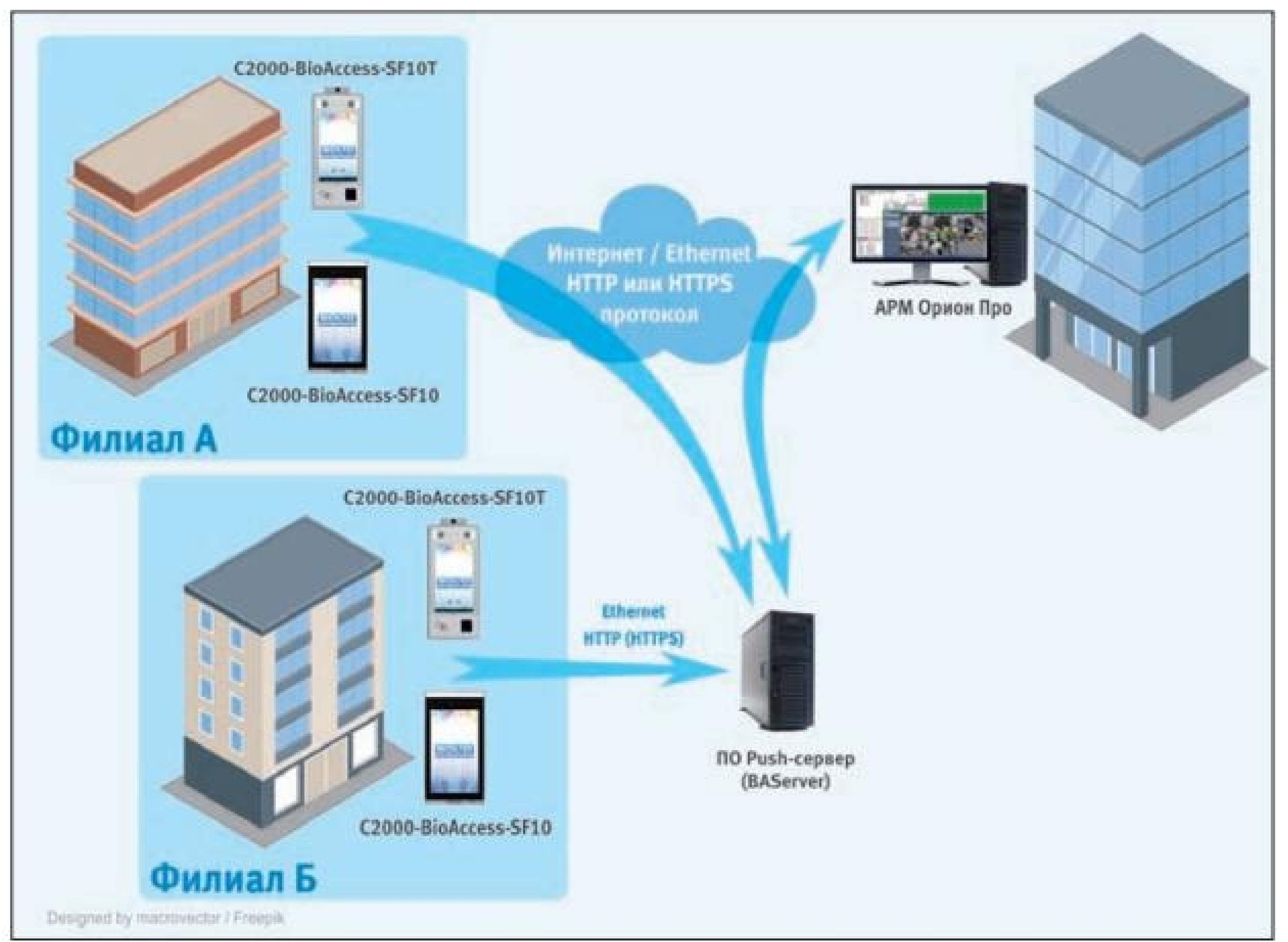


Рис. 3. Организация взаимодействия программных модулей АРМ "Орион Про" и биометрических контроллеров

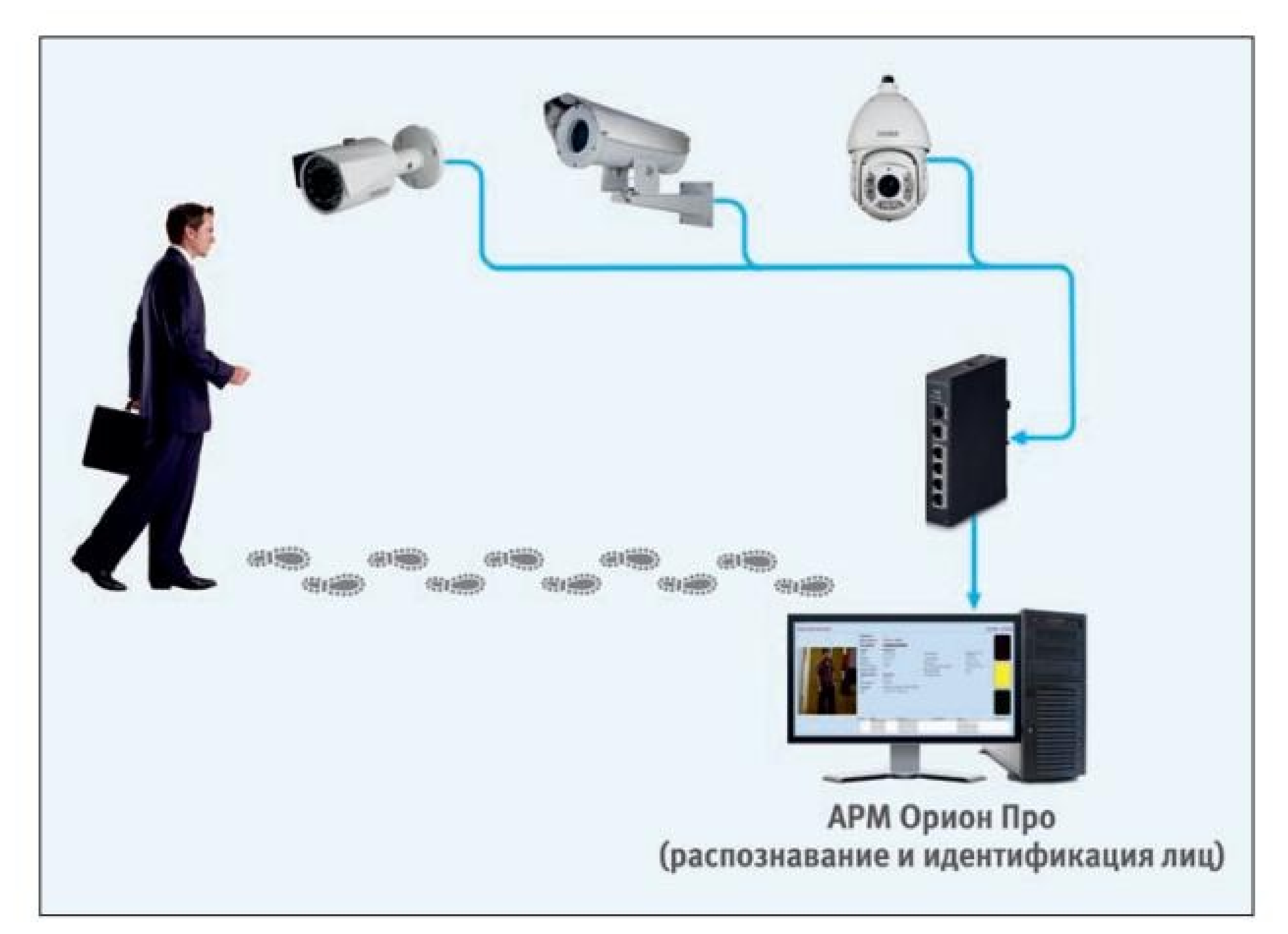


Рис. 4. Контроль передвижения сотрудника по объекту

Отличительные особенности Push-протокола:

- для организации связи между прибором и АРМ "Орион Про" используется протокол HTTP(S);
- инициатором связи является прибор – выступая в качестве клиента, контроллер посылает запросы на сервер по протоколу HTTP(S) и ожидает от него ответа.

Поддержка нового протокола в составе АРМ "Орион Про" позволяет:

- использовать для передачи данных незащищенные каналы связи, в частности Интернет;
- организовывать подключение приборов, расположенных в разных подсетях, через промежуточные прокси-серверы;
- строить более сложные (распределенные) системы, где компоненты, отвечающие за СКУД и связь с приборами, могут располагаться в разных сетях.

При построении распределенных систем программный модуль BAServer может размещаться как на одном, так и на нескольких компьютерах. Требования к размещению определяются балансировкой нагрузки, необходимостью использования защищенного соединения, сетевыми правилами безопасности и т.д. В приведенном на рис. 3 примере АРМ "Орион-Про" имеет доступ ко всем биометрическим контроллерам посредством программного модуля BAServer, расположенного в филиале В. При этом часть системы может иметь незащищенное HTTP-соединение (филиал В), другая часть системы может быть защищена HTTPS-соединением.

Программный модуль распознавания лиц

В АРМ "Орион Про" имеется и другая возможность распознавания и идентификации лиц – на изображениях, поступающих с сетевых видеокамер подсистемы видеонаблюдения. Для этого используется программное обеспечение "Распознавание лиц". С его помощью пользователь может организовать персональный видеоконтроль в охраняемом помещении или на территории. При этом видеокамеры могут работать в условиях низких температур, осадков, в вандалоопасных или даже во взрывоопасных зонах. Следует отметить, что в некоторых случаях распознавание через видеокамеры удобнее, так как программный модуль распознавания лиц допускает больший угол наклона головы, а сами камеры имеют более широкие допуски по температурному диапазону или способу установки, чем биометрические контроллеры.

В случае использования данного функционала для контроля и управления доступом в АРМ "Орион Про" предусмотрено событие "Сотрудник распознан". В свою очередь, в механизме сценариев имеется возможность предоставить или заблокировать доступ конкретному сотруднику (или нескольким). Таким образом, создав соответствующий сценарий и связав его с событием, можно создать управляющую команду для системы контроля и управления доступом ИСО "Орион" на базе контроллера "С2000-2" и организовать проход через дверь.

Видеофиксация перемещений

Другой вариант применения модуля распознавания лиц – контроль передвижения сотрудника по объекту (рис. 4).

Для организации видеофиксации перемещений конкретного человека также необходимо воспользоваться механизмом сценариев управления ИСО "Орион". Для получения необходимой информации достаточно заблаговременно организовать запись по событиям распознавания, чтобы затем при формировании отчета воспользоваться журналом событий. В нем можно отфильтровать ФИО необходимого сотрудника и проследить по всем камерам, где, в какое время и в каком месте он проходил.

Таким образом, новые технологии распознавания лиц представляют пользователям ИСО "Орион" новые перспективные возможности для построения комплексных систем безопасности и решения новых задач. ■

Газоаналитические системы для повышения безопасности метрополитенов

Метрополитены России ежедневно перевозят более 20 млн человек. Самый большой объем перевозок осуществляется Московским метрополитеном. Главная опасность метрополитена в том, что на этом подземном объекте в случае какого-либо инцидента, будь то авария, пожар, теракт или отключение напряжения, любой работник и пассажир становится заложником ситуации и без помощи успешная эвакуация может быть затруднительна



Александр Лукьянченко
Заместитель генерального директора ООО "ПГИ" по пожарной безопасности, к.т.н.



Леонид Волков
Заместитель генерального директора ООО "ПГИ" по техническим вопросам



Анна Столлер
Диспетчер службы оперативного обеспечения ФКУ ЦУКС ГУ МЧС России



Никита Лукьянченко
Наладчик КИПиА ООО "ПГИ"

Метрополитены – это предприятия, связанные с повышенной опасностью, уровень которой существенно возрастает в условиях возникновения аварии или пожара.

Статистика и опыт эксплуатации метрополитенов мира показывают, что это опасные, в том числе с противопожарной точки зрения, общественные объекты, большей частью работающие в подземных условиях с использованием стационарно смонтированных эскалаторов и являющиеся местами с массовым пребыванием людей.

Кроме того, метрополитены – сложные инженерно-технические сооружения, представляющие собой множество станций, объединенных сетью подземных тоннелей. При нарушении эксплуатационных правил, сбоях в работе по различным причинам, недостаточном уровне защиты от аварии или пожара, при возникновении даже одного очага возгорания они чрезвычайно уязвимы, так как удалены от поверхности и могут быть быстро задымлены, что может привести к массовой гибели пассажиров, работников и значительному материальному ущербу. Поэтому вопросам обеспечения безопасности на объектах метрополитенов всегда уделяется особое внимание как администрацией таких транспортных предприятий, так и сотрудниками подразделений.

Критерии опасности объектов метрополитена

Основные объекты в структуре метрополитена, которые представляют особую опасность, – электровозные депо, включающие в себя парк для отстоя, текущего ремонта, технического сервиса электровозов, вагонов поездов и мотовозов.

На территории метро размещены административно-бытовые, производственные, складские помещения, в том числе с хранением горючих жидкостей, горюче-смазочных, лакокрасочных материалов, используемых для топливной заправки мотовозов, проведения окрасочных работ при ремонте, обслуживании подвижного состава, а также электроподстанции, обеспечивающие электрическую тягу для поездов метро.

Станции метрополитена характеризуются большей частью подземными остановочными пунктами, состоящими из комплекса залов, переходов, лестниц, эскалаторов и помещений для обслуживания пассажиров, размещения инженерного оборудования, дежурного персонала.

Кабельные сооружения – тоннели, коллекторы, коридоры и технические этажи, шахты, отсеки, камеры предназначены для прокладки электрических трасс, монтажа соединительных муфт, свободного прохода обслуживающего персонала. Они характеризуются высоким уровнем пожарной нагрузки, а в часы пик только один поезд метро перевозит более 1 тыс. пассажиров.

Актуальность газового контроля в метро

Для повышения безопасности пассажиров и сооружений метрополитена с целью раннего обнаружения аварии или пожара целесообразно использовать современные системы газового контроля.

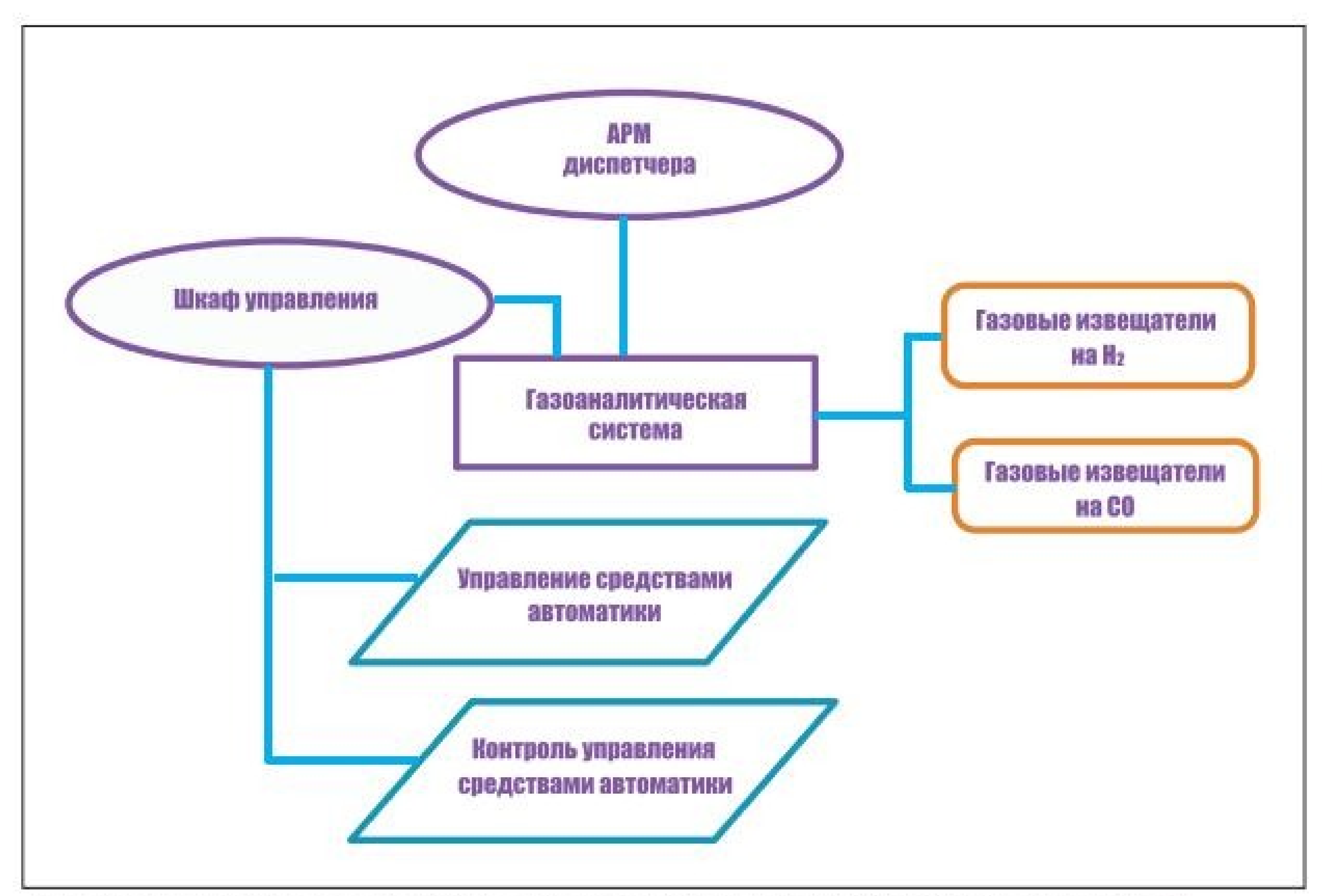
Статистика и опыт эксплуатации метрополитенов мира показывают, что это опасные, в том числе с противопожарной точки зрения, общественные объекты, большей частью работающие в подземных условиях с использованием стационарно смонтированных эскалаторов и являющиеся местами с массовым пребыванием людей

Работа по дальнейшему совершенствованию современных систем, а также отдельных технических средств раннего обнаружения аварий (загораний) является весьма актуальной ввиду:

- перехода предприятий и организаций к хозрасчетным отношениям;
- сокращения численности малоквалифицированной части обслуживающего персонала, обеспечивающего контролирующие функции;
- возрастания роли автоматизации производств;

Таблица. Выделение CO и H_2 при пиролизе различных материалов

Материал	Масса, г	Газовыделение, мг/г (грамм вещества)		Количество разлагающегося материала (г) в объеме 100 м³, фиксируемое ГИ	
		CO	H_2	CO	H_2
Дерево	0,1	444,6	93,6	0,224	0,534
Бумага	0,2	435,6	114,75	0,229	0,435
Изоляция электропроводки (ПВХ)	0,3	332,64	91,47	0,300	0,546



Структурная схема газоаналитической системы с интеграцией в общую систему АРМ оператора

Особенностью газового контроля является необходимость учета иногда очень сложной динамики движения газов, зависящей от многих параметров. В любых условиях и на любых объектах наблюдаются воздушные потоки, переносящие и перемешивающие газы, из-за чего их концентрация неоднородная и непрерывно меняется

- необходимости надежного обеспечения сохранности материальных ценностей (наиболее важная цель в нашей стране).

Применение нового класса газовых извещателей позволяет более комплексно строить систему безопасности объектов. Такие извещатели по своей конструкции не боятся запыленной атмосферы и высокой влажности, имеют газочувствительные элементы, которые могут регистрировать малые концентрации контролируемых газов.

Многочисленные исследования, проведенные для большого количества веществ, показывают, что закономерности их разложения существенно зависят не только от вида горючего, но и от температуры реакции, скорости ее изменения во времени, размеров пиролизуемого образца, его формы, степени распада, контакта с продуктами разложения и т.д.

Эффективность доказана

Перечень и количество газов, выделяющихся на начальной развивающейся аварийной ситуации, определяются составом материалов, включенных в этот процесс, однако в подавляющем большинстве случаев можно уверенно выделить основные характерные газовые компоненты, в частности водород и угарный газ. Представленные в таблице экспериментальные результаты исследований выделения водорода и оксида углерода в помещении при пиролизе таких широко использующихся материалов, как бумага, дерево и изоляция электропроводки, подтверждают физику процесса.

Приведенные экспериментальные данные доказывают, что газовые извещатели наиболее эффективны на начальной стадии образований опасных концентраций, обеспечивают достаточный запас времени для принятия мер по ликвидации аварийной ситуации (возгорания), а системы раннего обнаружения аварий должны ориентироваться на анализ двух газовых компонентов в атмосфере помещения – водорода H_2 и оксида углерода CO, большое количество которых выделяется именно на ранней стадии развития аварийной ситуации – пиролиза.

Так, в помещении объемом 100 куб. м будет достаточно использовать один газовый извещатель (без учета вентиляции и кондиционирования), который будет обеспечивать его безопасность. Термодеструкция у разных материалов начинается при различной температуре, но в любом случае она опережает появление дыма и пламени, процесс нагрева может быть медленным и длиться на протяжении десятков часов или дней. Высокая чувствительность к выделяющимся углеводородам, селективность и быстродействие газовых извещателей с уверенностью рассматриваются как основные преимущества при раннем обнаружении аварии с возможностью оценки экологической напряженности рабочей зоны в местах пребывания людей (при нормальном регламентном режиме работы технологического оборудования).

Быстрое диагностирование аварийной ситуации

При приеме идентифицированного сигнала газовый извещатель должен интеллектуально обработать поступивший параметр по пороговo-дифференциальному подходу, собственному интеллектуальному алгоритму, с настройкой на контролируемый параметр (по водороду и оксиду углерода), который позволяет достоверно оценить и диагностировать появление аварийной нарастающей ситуации, не учитывая появление или образование ложных показателей (образование локальных и кратковременных всплесков, незначительное нарастание концентрации газов за единицу времени, отсутствие одного из контролируемых газов, несоответствие процентного соотношения между выделяемыми газами и другими физическими и химическими показателями).

Структурная схема газоаналитической системы представлена на рисунке.

Данная система должна функционировать как самостоятельная и при необходимости интегрироваться в общую систему безопасности как элемент системы раннего обнаружения аварийных ситуаций до начала возникновения аварийных и пожаровзрывоопасных концентраций и состояний.

Учет воздушных потоков и экологический мониторинг

Анализ состава атмосферы контролируемого объекта позволяет оперативно контролировать аварийные ситуации на начальных стадиях при правильном подходе к методике измерения.

Выделение в атмосферу специфических газов происходит при самых различных процессах, и контроль этих газов означает контроль интересующих процессов.

Особенностью газового контроля является необходимость учета иногда очень сложной динамики движения газов, зависящей от многих параметров. В любых условиях и на любых объектах наблюдаются воздушные потоки, переносящие и перемешивающие газы, из-за чего их концентрация неоднородная и непрерывно меняется.

В задачи газоаналитической системы входит и экологический мониторинг, когда показания определяют средневзвешенное значение дозы токсичного вещества (CO), поглощающегося человеком в данном помещении, и техногенное отклонение показателя по H_2, при достижении дифференциального контролируемого значения которого нужно максимально быстро зарегистрировать появление опасного компонента и отреагировать на его появление путем оповещения ответственного персонала, включения или выключения (при необходимости) устройств автоматики. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Вопросы сопряжения комплексов технических средств оповещения различных производителей

Последнее десятилетие ознаменовалось большим количеством опытно-конструкторских разработок новых комплексов технических средств оповещения, а также модернизацией ранее созданных. 2020 год не стал исключением, поскольку в этот период прошли приемочные испытания с участием МЧС России два новых и один модернизированный комплекс. Очевидно, что возрастающий спрос на оборудование для построения систем оповещения будет подталкивать предприятия-изготовителей к созданию новых и расширению функциональных возможностей ранее созданных комплексов



Алла Леонова
Младший научный сотрудник
ФГБУ ВНИИ ГО ЧС МЧС России



Андрей Зуев
Генеральный директор
компании "Инфострата"

В 2015 г. в Российской Федерации был впервые введен национальный стандарт на создание технических средств оповещения [1], в соответствии с которым была проведена классификация и установлены основные требования для разработки и модернизации технических средств оповещения. Вместе с тем недостаточная проработанность требований в части сопряжения средств оповещения привела к отсутствию взаимодействия между производителями технических средств оповещения как на этапе разработки, так и на этапе запуска в серийное производство в части разработки протоколов взаимодействия между комплексами различных изготовителей, что породило их полную несовместимость.

Разность применяемых различными производителями протоколов информационного обмена и их несовместимость привели к проблемам при создании, модернизации или расширении систем оповещения населения. Сложилась такая ситуация, когда на территории одного субъекта Российской Федерации или муниципального образования может присутствовать несколько сегментов систем оповещения различных производителей, не обеспечивающих централизованное управление с одного терминала. Такая фрагментированность систем, а также перспектива использования более одного терминала управления на рабочем месте дежурного Единой дежурно-диспетчерской службы (ЕДДС) увеличивает время доведения сигналов оповещения по всей системе в целом.

Юридические, технические и экономические аспекты рассматриваемой темы

Как и любая разработка, протокол взаимодействия элементов системы оповещения (система команд; далее – протокол взаимодействия) часто является объектом интеллектуальной собственности разработчика комплекса технических средств оповещения или его производителя. Доступ к протоколу взаимодействия охраняется до тех пор, пока технические или экономические показатели не будут достигнуты или пересмотрены. Ситуация с охраной прав на использование протоколов уже давно ведется в юридической, а не технической сфере. При том, что оборудование практически всех марок различных производителей может на техническом уровне обеспечивать взаимодействие, отсутствует документальное подтверждение данного факта. Собственники протоколов юридически не разрешают их использование другим изготовителям технических средств оповещения. Естественно, основной причиной этому служат опасения, что конкуренты смогут занять ранее подготовленные производителем долгосрочные рынки сбыта. Одним из показательных примеров может служить ситуация, при которой производитель или его дилер выиграл конкурсные процедуры за цену ниже себестоимости работ (услуг) в надежде, что создание инфраструктуры пунктов управления системой оповещения на определенной территории в течение следующих нескольких лет позволит вернуть инвестиции за счет продажи оконечного оборудования. Аналогичный пример из бытовой сферы: к бритвенным станкам одного производителя подходят кассеты с лезвиями только этого производителя и не подходят другого. Часто компания-изготовитель продает сам станок со значительным дисконтом относительно его реальной стоимости с надеждой получить прибыль и вернуть инвестиции за счет долгосрочной продажи кассет. Что произойдет с его бизнес-планом, если завтра он разрешит безболезненно изготавливать другим производителям кассеты с таким же посадочным местом? Ответ очевиден. Таким образом, производители систем оповещения, создавая инфраструктуру пунктов управления, автоматически ограничивают использование оборудования других компаний ввиду невозможности их работы с протоколами ранее установленных устройств для оповещения.

Как решить проблему технического сопряжения средств оповещения разных производителей?

Требования по сопряжению технических средств оповещения различных производителей закреплены в п. 5.1.8 новой редакции ГОСТ Р 42.3.01–2021 "Гражданская оборона. Технические средства оповещения. Классификация. Общие технические требования", который вступит в действие с 01.06.2021 г. В частности, в данном национальном стандарте указывается, что технические средства оповещения различных производителей должны программно-технически сопрягаться напрямую или через устройства сопряжения, что должно быть подтверждено актом совместных испытаний с участием представителей федерального органа исполнительной власти, уполномоченного на решение задач в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, и полномочных представителей предприятий – изготовителей технических средств оповещения.

В случае осуществления разрешения на использование протокола одного производителя другому (или нескольким) разрешивший использование своего протокола производитель принимает на себя обязательства по его поддержке в работоспособном состоянии

В настоящее время имеются положительные примеры различных способов решения проблемы сопряжения технических средств оповещения различных производителей.

Конвертация протоколов взаимодействия

Первый и самый простой – это конвертация протоколов взаимодействия комплексов технических средств оповещения различных производителей. Как упоминалось ранее, проблема заключается не в технической части, а сугу-

бо в праве использования протоколов различных изготовителей. Частным случаем такого решения является принцип использования аппаратных модулей, выпускаемых собственником протокола в комплектах оборудования других производителей. Одним из удачных примеров реализации аппаратного сопряжения может выступать интеграция модуля, поддерживающего протокол П-166М, в оборудование СГС-22МЕ.

Второй способ – использование устройства сопряжения (конвертора протоколов). В качестве положительного опыта создания устройства сопряжения можно отметить разработанный ЗАО "Научно-производственная фирма "Сигма" (Калуга) блок сопряжения П-161М РММ-8 БС. Данный блок прошел приемочные испытания в 2016 г. и был рекомендован для обеспечения программно-аппаратного сопряжения между комплексами технических средств оповещения различных производителей. Вместе с тем высокая цена данного блока и, главное, время, прошедшее с момента его выпуска, сделали его практически нереализуемым. Это объясняется тем, что многие производители, обновив линейку продукции и программного обеспечения, не уведомили об этом разработчиков П-161М РММ-8 БС, из-за чего при заказе блока сопряжения вместо серийно выпускаемой продукции зачастую должен выпускаться индивидуальный продукт.

Разрешение на использование протокола и вытекающие из этого сложности

Имеется еще один способ сопряжения технических средств различных производителей. Как ранее уже упоминалось, технически не составляет труда расшифровать и воспроизвести протокол другого производителя, в связи с чем отдельные производители заявляют о возможности поддержки протоколов сторонних производителей, вводя тем самым в заблуждение конечных потребителей. Фактически, кроме незаконного использования чужого протокола и нарушения интеллектуальной собственности, данные действия могут вызвать и реальный риск выхода из строя системы оповещения не только объектового, но и муниципального и регионального уровней при внесении изменений производителем оборудования в протокол обмена. Здесь требуется более подробное пояснение. В случае осуществления разрешения на использование протокола одного производителя другому (или нескольким) разрешивший использование своего протокола производитель принимает на себя обязательства по его поддержке в работоспособном состоянии (например, путем сохранения или регулярного обновления). Поддержка также подразумевает согласованное и заблаговременное уведомление партнеров о внесении в протокол изменений, затрагивающих работу средств оповещения иных производителей. В случае отсутствия партнерских отношений собственник протокола вправе в любой момент времени изменить его структуру. Такое изменение может оказаться критическим для работы оборудования другого производителя, использующего данный протокол без разрешения собственника. Причем речь идет не о преднамеренном саботаже со стороны собственника протокола, а о планомерном обновлении политик безопасности. Оцените, сколько раз за последние полгода происходило автоматическое обновление программного обеспечения вашего персонального компьютера или смартфона! Регулярное, часто автоматическое, обновление программного обеспечения стало нормой во всех сегментах техники. Именно поэтому гораздо большим проступком, чем незаконный реверс-инжиниринг, является само использование протокола без разрешения и последующей поддержки правообладателя.

Являются ли выходом устройства сопряжения для конвертации протоколов?

Таким образом, любое использование устройств сопряжений, обеспечивающих конвертацию протоколов, не способно обеспечить полное соответствие прохождения полей команд/квитанций в обе стороны. Если подходить формально к вопросу сопряжения систем всех уровней, возникает коллизия следующего свойства: протокол каждого производителя имеет определенное количество полей для записи команд и квитанций о состоянии оборудования, и у каждого производителя этот набор команд/квитанций разный. Какой-то производитель ограничивается набором из 30 полей записи, а протоколы некоторых производителей включают в себя до 150 полей. Таким образом, выполнение требования о программном и техническом сопряжении формально невыполнимо ввиду несовпадения количества команд/квитанций двух разных производителей.

Опыт стандартизации в других областях применения электронной техники – выводы и рекомендации

Проблема множественности протоколов характерна практически для всех сфер электронной и телекоммуникационной техники, где имеется информационный вакуум или недостаточное регулирование. Многие сферы уже прошли данный этап и успешно пожинают плоды стандартизации и кросс-платформенности. Так происходило и со стандартами хранения информации, и с протоколами обмена в телекоммуникационной сфере и во многих других областях. Следовательно, если грамотно транспонировать опыт стандартизации обмена информацией из других областей в область систем оповещения населения, то появляется достаточно высокая вероятность получения положительного результата, обеспечивающего совместимость (аппаратно-программное сопряжение) оборудования различных производителей. При проведении стандартизации целесообразно избегать соблазна выбора протокола из числа уже применяющихся по мажоритарному принципу его применения. Не стоит также предпринимать попытки включить в состав универсального протокола все параметры, участвующие в информационном обмене протоколов всех производителей. Напротив, целесообразна разработка нового протокола с организацией как минимум двукратного запаса количества свободных полей. Это объясняется тем, что практически любой протокол обмена в системах оповещения состоит из двух типов данных – самого сообщения и служебной информации. В свою очередь, сообщение может содержать аудио-, аудиовизуальную или буквенно-цифровую информацию, а служебная информация быть представленной как командами и квитанциями, обеспечивающими работу самого протокола, так и командами, и квитанциями состояния элементов систем оповещения. Если попытаться классифицировать поля состояний каждого производителя, то условно их можно разделить на обязательные и вспомогательные. При этом к обязательным полям следует относить исполнение базовых наборов команд и отчет об их исполнении, а также квитанции о состоянии критически важных параметров системы. Остальные поля состояний следует принять как вспомогательные и не предъявлять требований к их обязательному соответствию у различных производителей. Такое разделение – это один из подходов к созданию единого (универсального) протокола [2].

Разработанные требования к единому протоколу должны стать обязательными для поддержки оборудования оповещения каждого производителя, что не отменяет поддержку производителем собственных проприетарных протоколов. Протоколы лицензируется каждым производителем на правах соблюдения им требований к их поддержке и к процессу производства оборудования.

Такой подход также позволит обеспечить гарантированное прохождение сигналов оповещения и полное программное и техническое сопряжение по основному набору команд всех систем оповещения на всех уровнях. В случае невозможности осуществить поддержку требований нового протокола более старыми модификациями технических средств производителям оборудования целесообразно предложить замену устройств систем оповещения или установку конвертера протокола.

Заключение

Как показывает мировая практика в области производства телекоммуникационного оборудования, использование стандартных универсальных протоколов позволяет существенно повысить стабильность работы сетей и систем связи и обеспечить совместимость оборудования различных производителей, что благоприятно сказывается не только на стоимости создания, но и на оперативности поиска замены в случае выхода оборудования из строя, что, в свою очередь, повышает готовность и устойчивость функционирования системы оповещения населения.

Список литературы:

1. ГОСТ Р 42.3.01–2014 "Гражданская оборона. Технические средства оповещения. Классификация. Общие технические требования": http://docs.cntd.ru/document/1200110556, дата обращения 01.03.2021.

2. Совместный приказ МЧС России и Минцифры России от 31.07.2020 № 578/365 "Об утверждении Положения о системе оповещения населения": http://docs.cntd.ru/document/565649076, дата обращения 01.03.2021. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Ложные тревоги и беспроводные СПС



До недавнего времени в нашей стране к ложным срабатываниям систем пожарной сигнализации (СПС) относились как к неизбежному злу, и это несмотря на то влияние, которое они оказывают на доверие людей к пожарным системам. Именно ложные срабатывания зачастую становятся причиной отключения систем пожарной автоматики на объектах.

В европейских странах этим вопросом обеспокоены давно, и в стандартах EN 54 предотвращению ложных тревог уделено большое внимание. Теперь не меньшее внимание к этому приковано и в наших нормах. Новый СП 484.1311500.2020 определяет инструменты борьбы с ложными тревогами. Новый ГОСТ на проектирование, монтаж, техническое обслуживание и ремонт, который вступит в силу уже в обозримом будущем, содержит четкие указания на случай возникновения ложных срабатываний СПС. Они предполагают, в зависимости от количества ложных тревог, замену части системы или даже системы целиком. И это может стать ударом по кошельку собственника.

Беспроводные системы имеют несколько способов защиты от ложных тревог. Одной из главных причин появления ложных извещений являются электромагнитные наводки на проводные линии связи извещателей с приемно-контрольным прибором. Радиоканальные пожарные системы гораздо более устойчивы к таким воздействиям ввиду отсутствия проводных линий. Некоторые системы устойчивы к помехам до третьей степени жесткости, а это уже промышленная установка. Еще одной причиной появления ложных тревог является накопление пыли, попадание в дымовую камеру мелких насекомых. И здесь, конечно, важны эффективные решения на уровне конструкции извещателей. С другой стороны, большое значение имеет наличие функции мониторинга технологических параметров пожарной системы, которая позволит контролировать ее состояние 24/7 и оптимизировать выезды на объект для технического обслуживания.

Современные беспроводные СПС в полной мере отвечают новым нормативным требованиям и обеспечивают высокий уровень пожарной безопасности объектов, позволяя своевременно и достоверно обнаружить пожар.

Михаил Левчук
Редактор рубрики "Беспроводные технологии", исполнительный директор ООО "Аргус-Спектр"

Ложные срабатывания СПС и как с ними бороться

Мы продолжаем цикл статей об изменениях нормативной базы в области пожарной безопасности (см. журналы "Системы безопасности" № 5/2020, № 6/2020 и № 1/2021). Рассмотрим следующее изменение нормативной базы, которое условно можно сформулировать как "Ложные срабатывания пожарной сигнализации"



Александр Зайцев
Независимый эксперт

Почему так актуальна тема ложных срабатываний в системах пожарной сигнализации (СПС)? Дело в том, что именно ложные срабатывания целые десятилетия заставляли повсеместно переводить исполнительные устройства пожарной автоматики из автоматического режима в ручной. Опыт этих десятилетий показал, что управлять исполнительными устройствами пожарной автоматики в ручном режиме нереально и делать это на объектах некому. Таким образом, автоматическому управлению в системе пожарной автоматики вряд ли можно что-то противопоставить. Но, чтобы оно оставалось именно автоматическим, надо максимально исключить ложные тревоги в СПС.

Что такое ложное срабатывание?

Согласно п. 6.1.1. СП 484.1311500.2020 новый свод правил ставит перед проектировщиками СПС две основные, но взаимоисключающие задачи:

- своевременное обнаружение пожара;
- достоверное обнаружение пожара.

С одной стороны, чем раньше произойдет обнаружение пожара, тем лучше. С другой – спешка вряд ли обеспечит требуемую вероятность достоверного обнаружения.

В п. 6.1.3. СП 484.1311500.2020 новый СП устанавливает требования по обеспечению достоверности обнаружения пожара.

Достоверность обнаружения должна достигаться комплексом следующих мероприятий:

- выбором типов пожарных извещателей;
- выбором алгоритма принятия решения о пожаре;
- защитой от ложных срабатываний.

Становится понятным, что борьба с ложными срабатываниями входит в список основных задач при проектировании СПС.

Ложное срабатывание (о пожаре) – извещение о пожаре, сформированное при отсутствии опасных факторов пожара (п. 3.21. СП 484.1311500.2020).

Это впервые появившееся в отечественной нормативной документации определение не дает в полной мере ответов на все вопросы. Попадают ли сюда срабатывания СПС как по преднамеренным, так и непреднамеренным причинам, вовсе не связанные с работой самой СПС? Курение, пыльные строительные работы? А если люди создают такие условия, что СПС не может не отреагировать, и тогда происходит ложный запуск исполнительных устройств пожарной автоматики?

Несмотря на то что основные причины ложных срабатываний уже были многократно проанализированы, позволю себе еще раз их привести:

1. Нарушение противопожарного режима (курение в неположенных местах).
2. Наличие пыли или тумана (пара) в контролируемых с помощью извещателей пожарных дымовых оптико-электронных точеных (ИПДОТ) помещениях.
3. Неправомочные действия при использовании ручных пожарных извещателей (ИПР).
4. Низкая защищенность от электромагнитных наводок:
   а) воздействие на линии связи;
   б) несоответствие степени защищенности по электромагнитной совместимости (ЭМС) применяемых технических средств для конкретных помещений, в которых они устанавливаются;
   в) ошибки в применяемых технических решениях.
5. Отсутствие технологических крышек на ИП во время проведения строительно-ремонтных работ.
6. Несвоевременное проведение ТО ИП.

Ложные срабатывания по вине ИПДОТ

Как показывает опыт, преобладающая часть ложных срабатываний происходит по вине ИПДОТ. Это наиболее используемый на сегодняшний день тип пожарного извещателя – более 95% от общего количества, и именно он является основным источником ложных срабатываний.

В соответствии с введенными требованиями к ИПДОТ за очень короткий период времени, с 1984 по 1997 г., пришлось понизить порог срабатываний до требуемого уровня, чтобы в конечном итоге пройти введенные в 2014 г. требования по огневым испытаниям с величины в 0,5 до 0,1 дБ/м. Но сделать действительно работоспособные и пригодные к своевременному и достоверному обнаружению возгораний

ИПДОТ сразу не получилось. Надо понимать, что снижение порога срабатывания произошло в первую очередь за счет снижения защищенности по ЭМС. Оказалось, что без дополнительных мер по защите от побочных явлений у существующих ИПДОТ есть большая вероятность ложных срабатываний от внешних электромагнитных помех, в том числе от элементарного включения освещения.

Пыль в ИПДОТ как источник ложных тревог

Почему в ИПДОТ может быстро скапливаться пыль, провоцирующая срабатывание ИП? По причине несовершенства конструкции корпуса, измерительной системы, попадания мелких насекомых и пр.

Но если постараться максимально защититься от пыли и насекомых, такой ИПДОТ никогда своевременно не обнаружит пожар.

Хороший ИПДОТ – это максимум компромиссов между отдельными составляющими конструкции, огромный объем всесторонних испытаний, хорошая элементная база со стабильными параметрами.

С учетом требований нового свода правил о необходимости еще на этапе проектирования закладывать технические решения по обеспечению максимальной вероятности достоверности, вопрос выбора конкретного типа ИП становится очень актуальным.

Линии связи между пожарными извещателями и ППКП

Проблема наведения электромагнитных помех на эту линию связи с воздействием на проводные неадресные и адресные ИП будет всегда актуальной, только решается она для таких систем по-разному.

В неадресных СПС выявление места ложного срабатывания – весьма трудозатратный процесс. В адресных СПС вопрос решается проще, а вероятность появления ложного срабатывания по указанной причине гораздо ниже. И уж совсем нереально по этой причине получить ложное срабатывание в беспроводных системах. Самый длинный проводник в них – антенна, но благодаря цифровой обработке поступающего от нее сигнала, ни одно внешнее электромагнитное воздействие не сможет вызвать ложное срабатывание ИП.



Рис. 2. Воздействие электромагнитной наводки на входные каскады ППКП

Ложные срабатывания по причине электромагнитных помех на входных каскадах ППКП

На рис. 2 представлен неадресный ШС длиной порядка 300 м, на котором возникла синфазная наводка. Попав на пожарный контрольно-приемный прибор (ППКП), с одного провода она уйдет на общую шину прибора или еще куда-то, в лучшем случае на заземление, а на втором – останется. Ее надо отправить на эту же общую шину или на заземление, ведь для принятия решения о пожаре нас интересует только постоянная составляющая тока в ШС. Что-то уйдет через входное сопротивление ППКП, но это будет зависеть от величины входного сопротивления ППКП со стороны шлейфа сигнализации. А оставшаяся большая часть? Лучше всего отправить ее на общую шину или на землю через низкое выходное сопротивление источника питания. Только он расположен еще в 100 м от ППКП, и на линию питания до ППКП тоже воздействуют внешние электромагнитные помехи. И эти помехи уже каким-то образом складываются на входе ППКП. Чего проще разместить источник питания возле или внутри ППКП, как часто делают во всем мире.

И сразу насчет входного сопротивления ППКП со стороны ШС.

В конце 90-х – начале 2000-х гг. на отечественном рынке было много охранно-пожарных неадресных ПКП малой и средней информационной емкости. Сконструированы они были для охранной сигнализации, но их использовали и для СПС. В целях удешевления этих ПКП в них были входы для ШС с высоким входным сопротивлением, вплоть до 10 кОм. С таким входным сопротивлением они, как хорошие детекторные приемники, собирали всевозможные электромагнитные воздействия. Наводки поступали и на ПКП, и на сами ИПДОТ.

Отмечу, что в адресных, как проводных, так и беспроводных СПС, такой проблемы не было, так как цифровые протоколы обмена изначально ее исключали.



Рис. 1. Конструктивные элементы ИПДОТ российского производителя

Выводы

В новом СП по проектированию мы получили только первую часть задач по исключению ложных срабатываний. Согласен, что пока никаких критериев оценки их предельной вероятности не приводится. Нет и полного перечня мероприятий по их исключению. Но так будет совсем недолго, надеюсь, что скоро вступит в силу новый стандарт, который восполнит недостающую часть. И тогда все проектно-монтажные организации вплотную столкнутся с обязательностью исключения такого негативного явления, как ложные срабатывания, а до тех пор следует руководствоваться теми рекомендациями, которые предусмотрены в новом СП.

Список литературы

1. Зайцев А.В., Неплохов И.Г. Ложные срабатывания в системах пожарной сигнализации. Части 1 и 2 // Системы безопасности. 2009. № 4, № 5.
2. Зайцев А.В. Большие проблемы маленьких ИПДОТ, или Попытка подвести итоги// Алгоритм Безопасности. 2015. № 2.
3. Зайцев А.В. Достоверность и своевременность обнаружения факторов пожара и попытка их учесть в нормах на СПС // Алгоритм Безопасности. 2016. № 2.
4. Зайцев А.В. Ложные срабатывания СПС, кто и как обязан с ними бороться // Алгоритм Безопасности. 2018. № 6. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Защита от ложных срабатываний в беспроводной системе пожарной сигнализации "СТРЕЛЕЦ-ПРО"

Введенные с 1 марта 2021 г. своды правил СП 484.1311500.2020, СП 485.1311500.2020, СП 486.1311500.2020 – первые документы из целого пакета новой нормативной базы пожарной безопасности. Одной из основных задач, поставленных при разработке новых требований, является сведение к минимуму количества ложных срабатываний систем пожарной сигнализации. Именно ложные срабатывания чаще всего становятся причиной отключения исполнительных устройств пожарной автоматики на объекте, оставляя его без автоматической защиты. И поэтому меры по их исключению или минимизации должны приниматься как на стадии проектирования системы, так и в процессе ее дальнейшей эксплуатации. В этой статье мы поговорим о преимуществах радиоканальной системы безопасности "Стрелец-ПРО" в борьбе с ложными срабатываниями.

1 марта 2021 г. вступил в силу новый свод правил по проектированию СП 484.1311500.2020 "Системы противопожарной защиты. Системы пожарной сигнализации и автоматизация систем противопожарной защиты. Нормы и правила проектирования". Радиоканальная система "Стрелец-ПРО" готова к изменениям в законодательстве и полностью соответствует новым нормативным требованиям по пожарной безопасности

Источниками ложных срабатываний в подавляющем большинстве случаев являются дымовые точечные извещатели. К причинам возникновения ложных срабатываний, как правило, относятся:

1) нарушение противопожарного режима (курение в неположенных местах и т.д.);

2) наличие пыли или пара в контролируемых с помощью дымовых извещателей помещениях (выбор типа пожарного извещателя при проектировании не соответствует назначению помещения);

3) проведение строительно-ремонтных или других пыльных работ на объекте без принятия мер по защите пожарных извещателей;

4) запыленность дымовых извещателей вследствие несвоевременного проведения технического обслуживания;

5) низкая защищенность от электромагнитных наводок.

В отличие от первых четырех причин, при которых система пожарной сигнализации честно выполняет свою функцию, ложные срабатывания от воздействия электромагнитных наводок – последствие некорректной работы системы пожарной сигнализации. Наведенное электромагнитной помехой напряжение пропорционально длине участка проводной линии, на который эта помеха воздействует. Поэтому сильнее всего подвержены воздействию электромагнитных наводок проводные системы, в которых кабельная линия является своего рода антенной. К примеру, воздействие помехи с напряженностью магнитного поля 30 В/м на участок линии, составляющий 10% от общей длины линии 20 м, создаст напряжение в линии 60 В, что приведет либо к ложному срабатыванию, либо к неисправности прибора. Это вызовет необходимость применения более дорогого экранированного кабеля, кабеля типа "витая пара", оптоволоконных линий связи.

Устойчивость "СТРЕЛЬЦА-ПРО" к электромагнитным наводкам

Радиосистема безопасности "Стрелец-ПРО" намного меньше подвержена воздействию внешних электромагнитных наводок. Единственный проводник в извещателях и контроллерах "Стрельца-ПРО" – это антенны длиной 5 см, поэтому при воздействии магнитного поля с той же напряженностью величина наведенного напряжения составит 1,5 В, причем воздействует помеха только на входную цепь приемника извещателя, что ни при каких обстоятельствах не способно привести к ложному срабатыванию (см. рис. 1).

Устойчивость оборудования радиосистемы "Стрелец-ПРО" к электромагнитным помехам подтверждена испытаниями 3-й степени жесткости по ГОСТ Р 50009–2000 и ГОСТ Р 53325–2012



Рис. 1. Зависимость величины наведенного напряжения от длины проводника



Рис. 2 Контроль аналоговых значений извещателей в ПО "Стрелец-Мастер" и "АРМ Стрелец-Интеграл"



Рис. 3. Уникальная конструкция извещателей серии "Аврора-ПРО"

Контроль запыленности дымовых камер

Отсутствие своевременного обслуживания извещателей и, как следствие, их повышенная запыленность – еще одна распространенная причина возникновения ложных срабатываний.

В радиосистеме "Стрелец-ПРО" предусмотрены мониторинг технического состояния извещателей и передача в режиме реального времени их аналоговых значений, в том числе и степени запыленности дымовых камер извещателей. При достижении критического значения запыленности извещатель передает сообщение о неисправности (см. рис. 2)

Эта функция доступна в ПО "Стрелец-Мастер" и "АРМ Стрелец-Интеграл". Она позволяет удаленно контролировать уровень запыленности всех извещателей. При необходимости можно отсортировать их по уровню запыленности и вывести вперед те извещатели, которые в первую очередь требуют обслуживания. А графическое отображение истории изменения параметров позволяет спланировать обслуживание заблаговременно.

Уникальная конструкция извещателей серии "АВРОРА-ПРО"

Корпус извещателей серии "Аврора-ПРО" из состава радиосистемы "Стрелец-ПРО" спроектирован таким образом, чтобы свести к минимуму вероятность ложных срабатываний. В нем предусмотрено два пылесборника, в которых оседает большая часть пыли, не достигая чувствительных элементов в дымовой камере. Защитная сетка в конструкции корпуса извещателей линейки "Аврора-ПРО" предотвращает попадание любых мелких предметов или насекомых внутрь, которые тоже могут привести к ложной тревоге.

Нередко причиной ложного срабатывания оптико-электронных дымовых извещателей является "засветка". Лучи света из внешних источников попадают на фотоприемник оптопары, создавая световые шумы, которые могут вызвать срабатывание извещателя. Для предотвращения "засветки" в корпусе дымовых извещателей линейки "Аврора-ПРО" имеется система отражателей, исключающая возможность попадания внешнего освещения на светочувствительные элементы (см. рис. 3).

Алгоритмы принятия решения о пожаре

Одно из рекомендуемых в СП 484.1311500.2020 мероприятий по защите от ложных срабатываний – применение в системах пожарной сигнализации алгоритмов принятия решения о пожаре В и С, описанных в этом же своде правил:

- 6.4.3. Алгоритм В должен выполняться при срабатывании автоматического ИП и дальнейшем повторном срабатывании этого же ИП или другого автоматического ИП той же ЗКПС за время не более 60 с, при этом повторное срабатывание должно осуществляться после процедуры автоматического перезапроса. В качестве ИП для данного алгоритма могут применяться автоматические ИП любого типа при условии информационной и электрической совместимости для корректного выполнения процедуры перезапроса.
- 6.4.4. Алгоритм С должен выполняться при срабатывании одного автоматического ИП и дальнейшем срабатывании другого автоматического ИП той же или другой ЗКПС, расположенного в этом помещении.

В системе "Стрелец-ПРО" с применением функции пожарных извещателей "Двухкратное срабатывание в течение 60 с" реализуется алгоритм В, а функция зон контроля "Пожар по двум адресам в зоне" позволяет реализовать алгоритм С

4 фактора эффективности

Следующие факторы позволяют радиоканальной системе пожарной сигнализации "Стрелец-ПРО" свести к минимуму уровень ложных тревог на объекте:

1. Пожарные извещатели радиосистемы "Стрелец-ПРО" устойчивы к воздействию электромагнитных наводок.
2. Контроль уровня запыленности дымовых камер извещателей серии "Аврора-ПРО" позволяет заблаговременно предупредить о повышении запыленности каждого извещателя и необходимости обслуживания системы.
3. Уникальная конструкция защищает извещатели серии "Аврора-ПРО" от попадания внутрь пыли, мелких предметов и света, которые могут спровоцировать ложное срабатывание.
4. Радиосистема "Стрелец-ПРО" поддерживает работу алгоритмов В и С, предполагающих подтверждение пожарной тревоги срабатыванием двух извещателей или повторным срабатыванием одного. ■



Иду туда, не знаю куда?



В бизнесе новый день постоянно ставит новые задачи. Иногда их количество и требуемая скорость решения становятся нереальным по сложности вызовом и требуют мобилизации всех ресурсов как отдельных сотрудников компании, так и всей команды в целом. В такой ситуации "на коне" обычно оказываются те, кто достаточно мобилен и способен правильно оценить стремительно меняющуюся конъюнктуру.

Резко меняющиеся риски приводят к бешеному росту некоторых сегментов рынка систем безопасности. Это касается как старых, неторопливо развивающихся направлений, так и абсолютно новых, возникших только вчера. К сожалению, последние месяцы регулярно сталкиваюсь с тем, что мощная волна перемен выносит на гребень много "пены", которая залепляет потребителям глаза и уши. Дорогие заказчики, партнеры, клиенты, быстро купленное первое попавшееся не значит нужное и хорошее. Уж сколько раз твердили миру: неправильно определенные цели и сформулированные задачи приводят в итоге к восхитительно ненужному и бесполезному результату. Получается как в сказке: иду туда, не знаю куда, найду то, не знаю что.

Для начала определитесь, что вам надо, какие задачи имеют высший приоритет и какой результат вы хотите получить в итоге. Мы, разработчики, производители, проектировщики и инсталляторы, готовы помочь вам, но решить это, по большому счету, можете только вы.

Яркой иллюстрацией является ситуация с биометрическими СКУД. Направление, которое уверенно росло в последние годы, вдруг стремительно рвануло вверх. Резкая потребность в бесконтактных технологиях идентификации привела к взрывному росту бесконтактной биометрии, например на основе технологий сканирования лица с использованием нейроалгоритмов. На рынке стали появляться непонятные компании с сырыми разработками, цель которых – снять сливки и свалить. В этой ситуации можно только напомнить прописные истины. Вендор должен быть надежен и доступен, техническое задание должно быть четкое и прозрачное, планы развития должны быть прописаны на перспективу, если необходима интеграция с другими системами, она должна быть сформулирована заранее, программное обеспечение должно иметь требуемый функционал и входить в реестр Минкомсвязи.

Не делайте грубых ошибок, удачи!

Алексей Гинце

Редактор раздела "Системы контроля и управления доступом"

Управление гостевыми пропусками в современном бизнес-центре

Театр начинается с вешалки, а посещение бизнес-центра – с проходной. Чтобы создать позитивный настой у партнеров, клиентов, гостей, оформление временного доступа таким посетителям должно быть максимально комфортным. Современные средства идентификации и специализированное программное обеспечение для бюро пропусков позволяют решить эту задачу



Александр Фомин

Руководитель отдела автоматизации бизнес-процессов компании "ААМ Системз"

Как часто приходилось вам стоять в очереди в бюро пропусков для получения разового пропуска? Или заполнять свои данные вручную в журнале для посетителей? А может, ожидать посетителя на встречу, заполнять заявки на пропуск и все равно попадать в неудобную ситуацию, когда заявка "зависла" на каком-либо из этапов длинной цепочки согласований? К сожалению, до сих пор это довольно распространенное описание типовой проходной многих бизнес-центров. Согласитесь, что во время повсеместного внедрения ИТ-технологий не только в сфере безопасности, но и в повседневной жизни такая ситуация выглядит абсурдной. Наш отпечаток пальца является паролем к смартфону и ноутбуку, голос и лицо позволяют воспользоваться банкоматом, а мобильные приложения и интернет-порталы позволяют быстро получить государственные и муниципальные услуги. Можно ли сделать таким же удобным и безопасным доступ посетителей на проходной современной компании, банка, бизнес-центра, завода?..

Отличия гостевого пропуска от постоянного

Вернемся к управлению гостевыми и разовыми пропусками на объектах с большим ежедневным потоком людей, среди которых курьеры, обслуживающий персонал, клиенты, партнеры и т.д. Для этого сначала уточним, чем гостевой пропуск отличается от постоянного пропуска сотрудника, прошедшего "полный" путь для его получения, от HR до службы безопасности?

Во-первых, это короткий срок активации – от нескольких часов до нескольких дней. Если постоянный пропуск оформляется на достаточно продолжительный срок или деактивируется при увольнении сотрудника, то гостевой пропуск заказывается на конкретный промежуток времени.

Во-вторых, сама концепция разового или гостевого пропуска подразумевает, что посетитель приходит на ваш объект без карты доступа и заранее или дистанционно выдать ее не представляется возможным. Таким образом, первое, куда попадает каждый посетитель, – очередь в бюро пропусков с последующим заполнением документов.

В-третьих, физические карты доступа, как гостевые, так и постоянные, одинаково подвержены износу или утере. Но поскольку, как правило, гостевых и разовых карт неоднократно выдается и используется больше, это влечет серьезные материальные издержки, тем большие, чем крупнее компания. Эта проблема наиболее актуальна для объектов, использующих современные защищенные смарт-карты с многоступенчатой защитой, стоимость которых выше, чем незащищенных Proximity-карт. Для снижения издержек содержания гостевых пропусков некоторые компании применяют практику разделения типов носителей идентификаторов: для сотрудников используются защищенные и дорогие, а для гостевых пропусков незащищенные и дешевые карты. Однако очевидно, что это снижает защищенность объекта.

Специфика ПО для бюро пропусков

В чем отличие стандартной картотеки, имеющейся в программном обеспечении (ПО) системы контроля и управления доступом (СКУД), от



Рис. 1. Инфракрасный считыватель на проходной определяет посетителя по QR-коду

картотеки в специализированном ПО для бюро пропусков? Наиболее современные контроллеры СКУД позволяют на аппаратном уровне назначать дату и время активации и деактивации карты вплоть до минут и секунд. Однако это неудобно для разовых пропусков, учитывая высокую скорость их ротации, в отличие от пропусков постоянных сотрудников. Программное обеспечение позволяет быстро и, главное, удобно работать с данными параметрами. К тому же стандартные приложения картотеки в программном обеспечении для управления СКУД имеют большое количество настроек, относящихся к владельцу карты, которые избыточны и даже не нужны для сотрудника стандартного бюро пропусков, так как их использование ведет к неоправданным затратам времени и увеличивает вероятность ошибки при выдаче посетительских карт.

Процесс согласования гостевых заявок в крупных компаниях часто регламентируется корпоративными стандартами. На него также могут влиять уже внедренные решения, интеграцию которых с системами СКУД нужно постоянно поддерживать либо их разработкой только предстоит заняться. Кроме того, такие цепочки согласований могут быть весьма длинными и вариативными в зависимости от структуры и иерархии подразделений.



Рис. 2. Пример электронной заявки на выдачу временного пропуска

Итак, мы обозначили целый перечень еще далеко не всех проблем, с которыми ежедневно сталкиваются посетители, сотрудники, служба безопасности и руководители компаний и бизнес-центров при оформлении и выдаче гостевых и разовых пропусков. Для их решения и управления временными пропусками существуют специализированные программные комплексы.

Способы идентификации посетителей

Наиболее современные версии такого ПО представляют собой веб-приложения, позволяющие

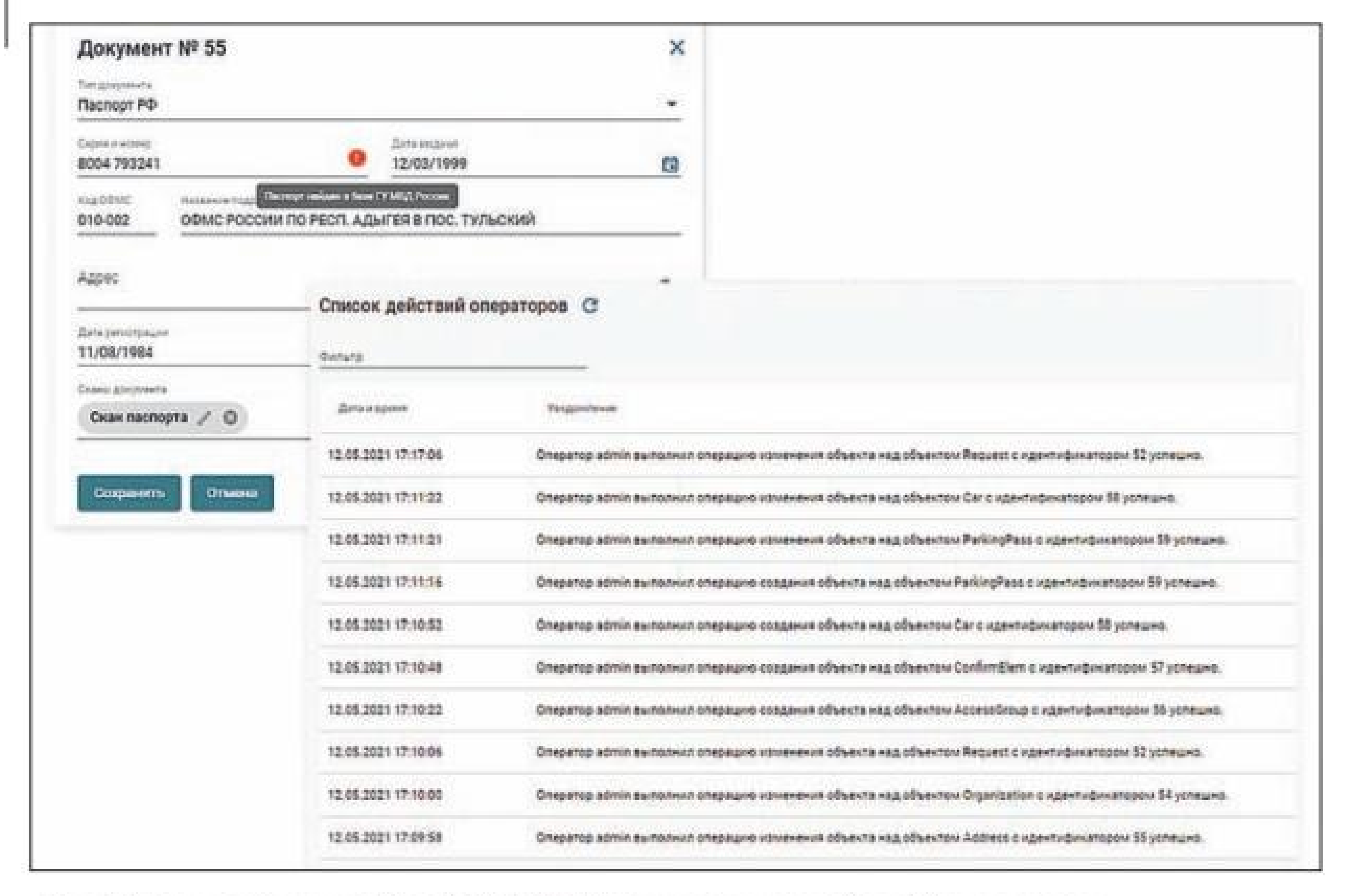


Рис. 3. Пример сверки с базой ГУ МВД России и аудита действий операторов

быстро и удобно заказать пропуск при помощи браузера или мобильного телефона. Программное обеспечение бюро пропусков может работать как самостоятельно в режиме электронного журнала, так и быть интегрированным с существующей на объекте СКУД и системами распознавания автомобильных номеров.

В таких системах в качестве идентификатора посетителя может использоваться также биометрия, например фотография посетителя, сделанная и отправленная заранее со смартфона либо отсканированная из документа, удостоверяющего личность. Фото лица загружается в систему, и по нему строится биометрический шаблон, а терминалы распознавания лиц, установленные в турникетной зоне, идентифицируют посетителя и при наличии соответствующих прав предоставят доступ. В настоящее время существуют терминалы, позволяющие одновременно измерять температуру посетителя и проверять наличие маски. Не таким функциональным, но не менее удобным и более дешевым вариантом гостевого идентификатора может быть QR-код, отправленный посетителю заранее. На таком приглашении указывается дата и время визита, а также любая дополнительная информация. Установленные на проходной инфракрасные считыватели позволяют считать закодированный идентификатор и передать его в контроллер СКУД.

Преимущества электронной системы выдачи временных пропусков

Давайте посмотрим на то, как выглядит работа с системой электронного заказа пропусков со стороны сотрудника, оформляющего гостевой пропуск для своего посетителя. Вместо устаревшего и неудобного способа заполнения печатных форм документов, контроля за согласованием на всех необходимых уровнях вплоть до получения заявки непосредственно на посту охраны современная система позволяет удобно, просто и быстро создать заявку в личном кабинете веб-приложения бюро пропусков. При этом можно ускорить процесс, используя автозаполнение уже известных данных (при повторном визите посетителя), создание групповых заявок, указание цели визита и прочей дополнительной информации, а также назначить лиц, согласование с которыми требуется. После каждого изменения статуса согласований, а также при приходе посетителя сотрудник получит мгновенную обратную связь – уведомление, использующее различные каналы связи: e-mail, СМС и мессенджеры.

Сотрудник бюро пропусков бизнес-центра, находящийся в зоне ресепшен, при визите посетителя получит всю нужную информацию из согласованной заявки. Как правило, рассматриваемые системы имеют интеграцию с сканерами распознавания и верификации документов, поэтому недостающую в заявке информацию можно быстро добавить в автоматическом режиме, и останется лишь выдать пропуск.

В том случае, если используются терминалы для распознавания лиц или QR-коды в качестве идентификаторов, вмешательство сотрудников зоны ресепшен в процесс гостевого доступа можно минимизировать и даже вообще исключить. Такой сценарий может выглядеть как потенциальная проблема в системе безопасности, но это не так: комбинирование стандартного функционала СКУД в виде модуля "Проходная", когда на экране показывается лицо и информация о человеке, совершившем проход, позволяют охране дополнительно верифицировать посетителей.

В качестве дополнительных средств безопасности при оформлении заявок применяются интеграции с черным списком утерянных и просроченных паспортов ФМС, внутренним черным списком бизнес-центра, а системы управления полномочиями операторов и ведения аудита их действий позволяют сделать систему прозрачной для службы безопасности.

Выгода и удобство, которые отмечают руководители крупных объектов, заключаются в наглядных данных в виде отчетов о количестве и интенсивности гостевых посещений тех или иных подразделений или арендаторов. Это позволяет получать важные статистические данные, анализ которых позволяет эффективнее управлять всем объектом. Снижается время, которое сотрудники вынуждены тратить на оформление стандартных процедур для гостевых заявок. Электронные системы управления гостевыми и разовыми пропусками позволяют автоматизировать выполнение требований 152-ФЗ, относящихся к хранению персональных данных. Это достигается путем удаления по установленному расписанию данных посетителей, сохраненных в базе данных. В случае если необходимо подписание бумажного согласия об обработке персональных данных, его возможно распечатать, используя заданный шаблон и автоматическую подстановку информации.

Производительность, наглядность, безопасность и позитивный настрой

Важнейшая составляющая любого успешного бизнеса – посетители, клиенты, партнеры. Нужно создать им позитивное настроение, ощущение поддержки, понимание того, что их временем дорожат, уже на входе. Использование современной и удобной системы, позволяющей максимально ускорить и автоматизировать оформление документов в бюро пропусков, свести к минимуму ожидание и очереди или совсем избавиться от такого понятия, как ресепшен, используя идентификацию по лицу или QR-коду, значительно повышает престиж организации как современной компании, формируя позитивные впечатления с первой встречи.

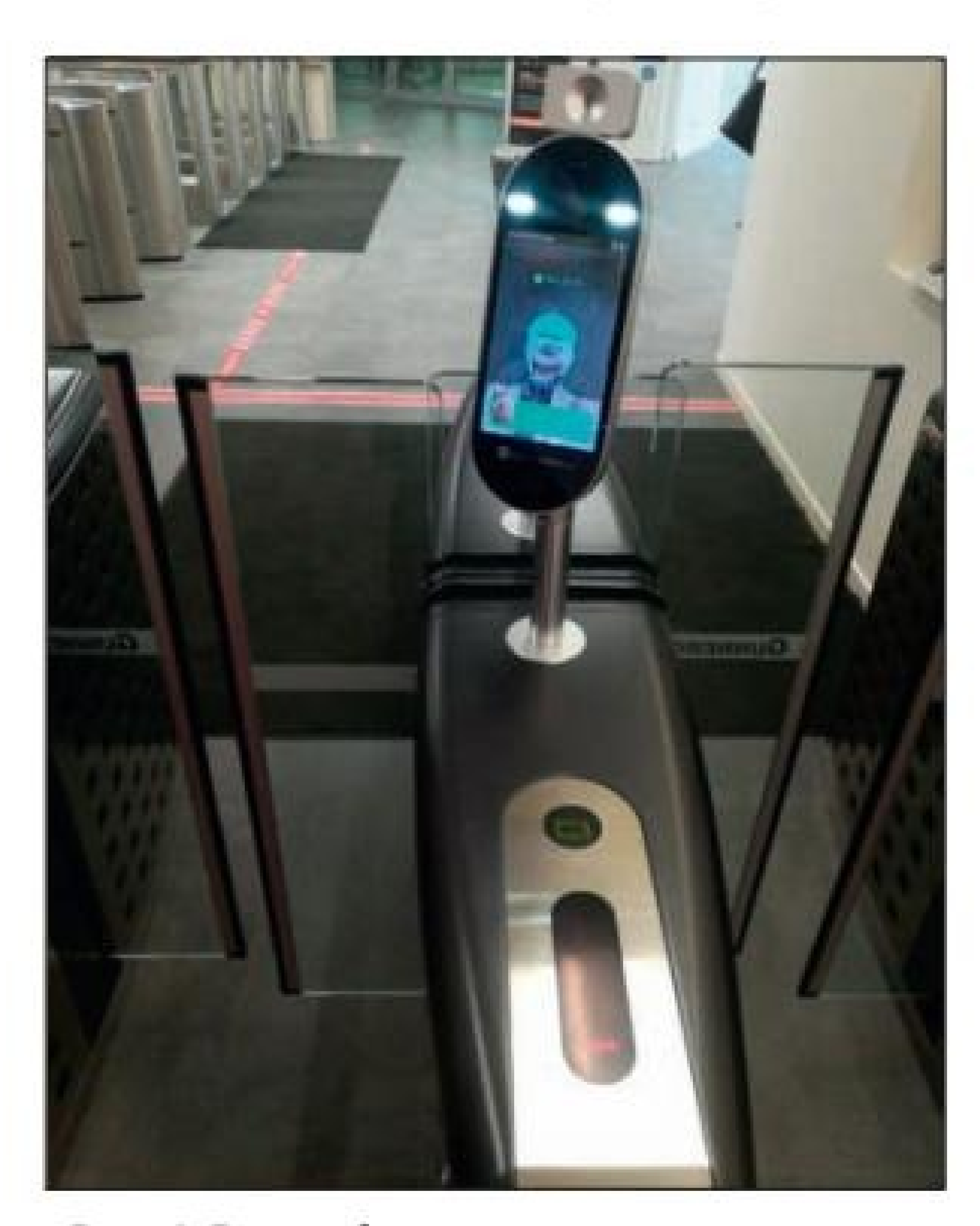


Рис. 4. Вход в бизнес-центр

Информационные системы в настоящий момент являются связующим звеном между всеми компонентами бизнеса, но скорость развития компании определяется быстродействием самого медленного элемента корпоративной инфраструктуры. Новые подходы и инструменты для управления гостевым доступом позволяют значительно увеличить производительность, безопасность и наглядность всех процессов, происходящих в компании, и мы уверены, что бумажные журналы уже очень скоро уйдут в прошлое. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Алексей Колосков
Заместитель начальника отдела
ФКУ "НИЦ "Охрана" Росгвардии



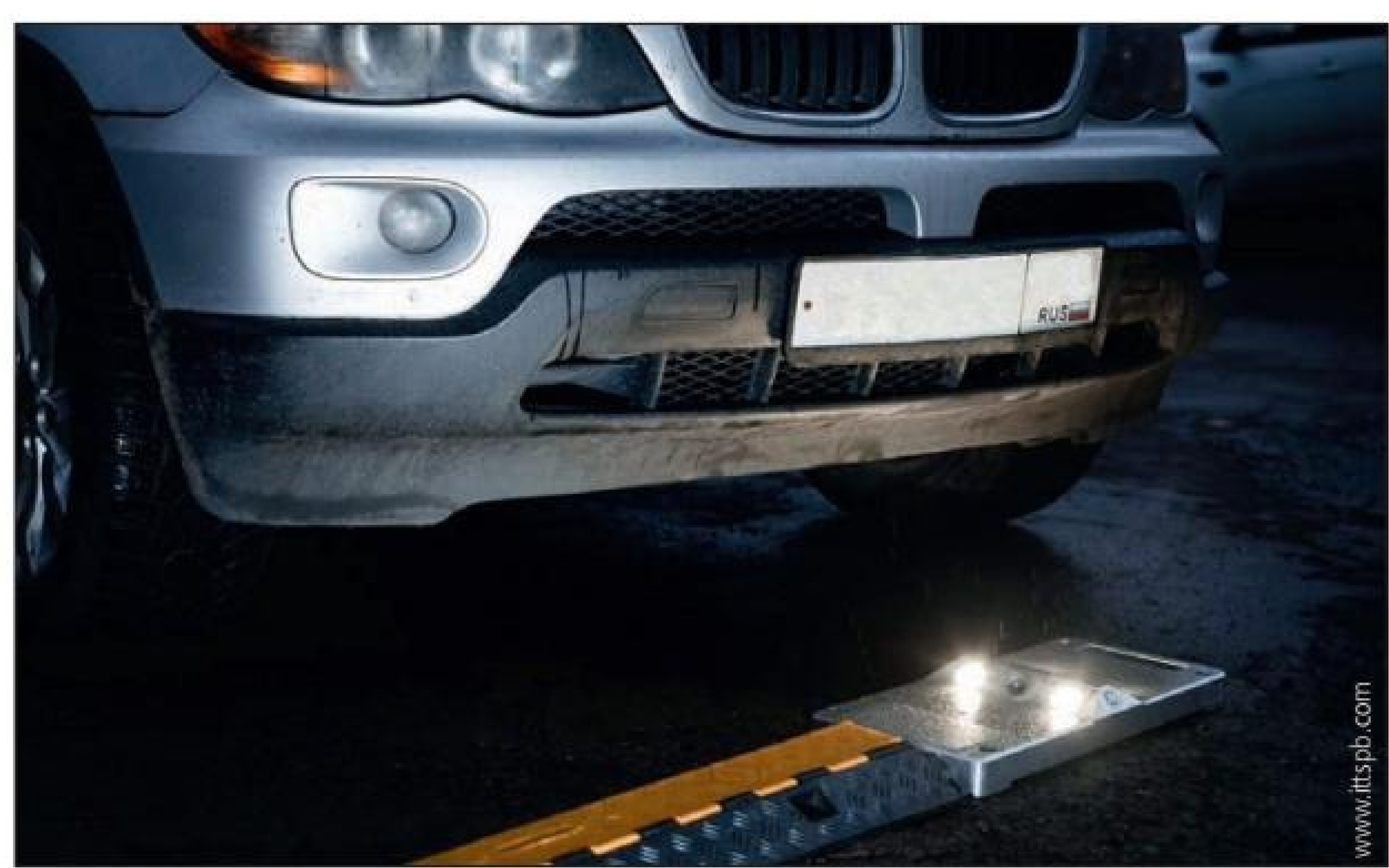
Марина Дворкина
Начальник сектора
ФКУ "НИЦ "Охрана" Росгвардии



Анатолий Вихирев
Научный сотрудник
ФКУ "НИЦ "Охрана" Росгвардии

Системы досмотра днища автотранспортных средств: классификация и состав

При обеспечении безопасности объектов и территорий особое внимание уделяется проведению тщательного досмотра, исключающего несанкционированный пронос или провоз предметов и веществ через точку доступа (контрольно-пропускной пункт). Применяемые технические и специальные средства позволяют с достаточно высокой эффективностью выявлять запрещенные для проноса/провоза предметы и вещества



Изучение опыта проведения досмотра автотранспортных средств показало, что для сокрытия предметов и веществ часто используется днище кузова, что позволяет производить действия криминальной и террористической направленности по сокрытию предметов и веществ лицам, не имеющим специальной подготовки.

При этом эффективному проведению непосредственного досмотра препятствуют следующие факторы:

1) труднодоступность расположения днища кузова;
2) недостаточность освещенности;
3) наличие большого количества штатно установленных деталей и узлов автотранспортного средства;
4) подверженность открытых поверхностей днища загрязнению, обледенению и воздействию других внешних неблагоприятных факторов.

Степени досмотра

Можно выделить четыре степени процесса досмотра днища автотранспортного средства (см. табл.).

Необходимость обеспечения качественного досмотра днища автотранспортного средства предъявляет особые требования к технической оснащенности контрольно-пропускных пунктов и проведению комплекса организационно-технических мероприятий.

Визуальный и инструментальный досмотр днища требует полной остановки (а при необходимости – и фиксации) автотранспортного средства на весь период проведения досмотра, что сопряжено с повышением трудоемкости процесса и негативно сказывается на пропускной способности. Следует учитывать и человеческий фактор. Кроме того, указанные способы досмотра днища не исключают возможности оказания негативного физического воздействия на оператора, производящего досмотр, например при срабатывании скрытно установленного взрывного устройства.

Автоматизированный досмотр позволяет переложить часть функций на систему, однако этому способу тоже присущи недостатки, характерные

Таблица. Степени процесса досмотра днища автотранспортного средства

Способ досмотра	Метод досмотра
1. Визуальный	Досмотр осуществляется оператором без использования вспомогательного оборудования или средств автоматизации
2. Инструментальный	Досмотр осуществляется оператором с использованием ограниченного набора вспомогательного оборудования
3. Автоматизированный	Досмотр осуществляется оператором с использованием средств автоматизации, обеспечивающих выполнение одного или нескольких этапов процесса досмотра
4. Автоматический	Проведение всех этапов процесса досмотра осуществляется средствами автоматизации без необходимости вмешательства оператора

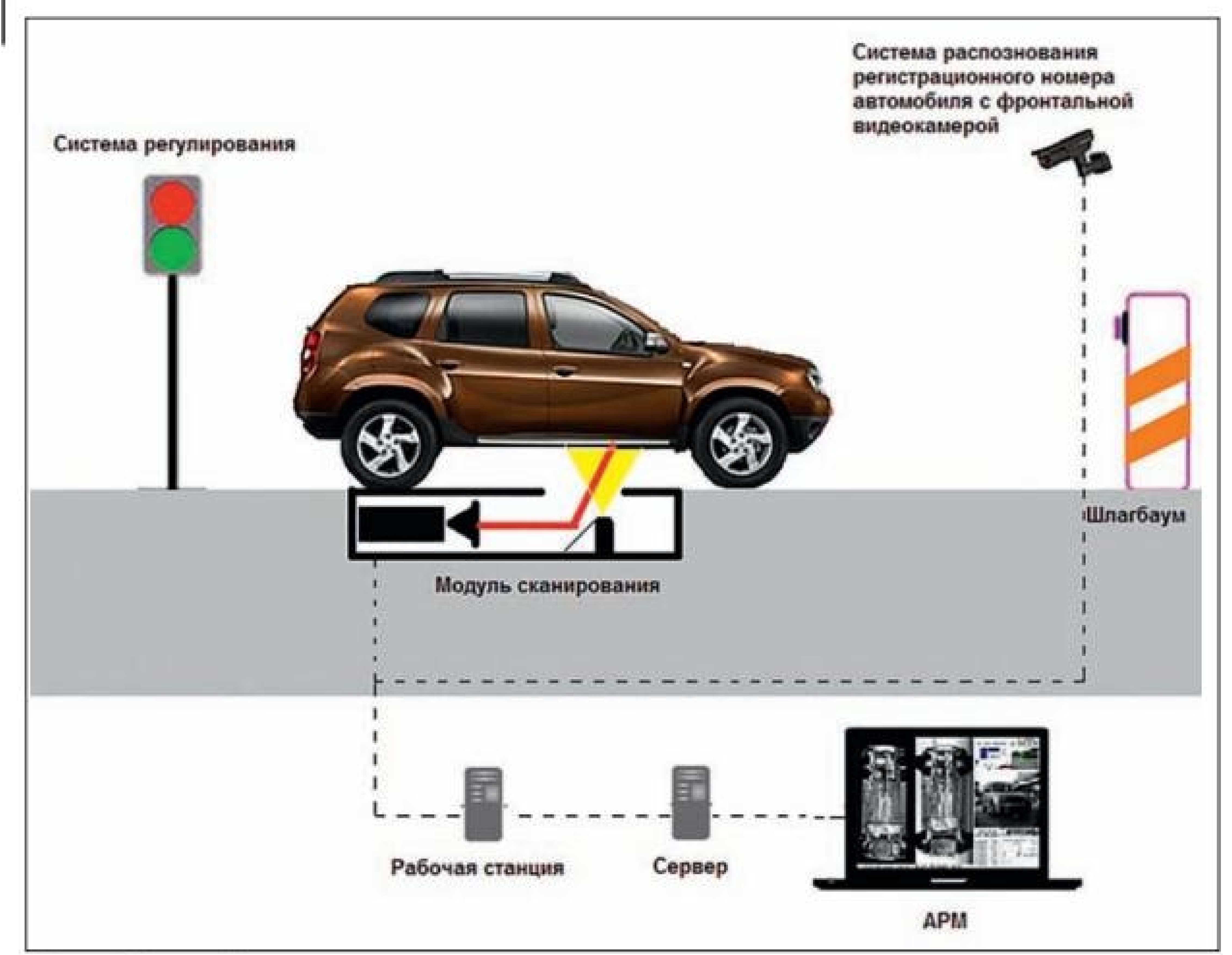


Рис. 1. Типовой состав и структура автоматизированных и автоматических систем досмотра днища автотранспортных средств

для визуального и инструментального досмотра, – низкая пропускная способность и наличие угрозы физического воздействия.

Наиболее оптимальным решением с точки зрения повышения надежности обеспечения безопасности операторов и увеличения пропускной способности контрольно-пропускных пунктов является применение высокоавтоматизированных систем досмотра, которые выполняют все стадии досмотра в автоматическом режиме с правом принятия оператором окончательного решения по санкционированию доступа.

Что входит в автоматизированную систему?

На отечественном рынке представлено множество автоматизированных и автоматических систем досмотра днища автотранспортных средств, в том числе не требующих остановки автотранспортного средства для проведения досмотра. Типовой состав и структура таких систем приведены на рис. 1.

Базовый состав такой системы включает в себя следующие компоненты:

1. Модуль сканирования, предназначенный для производства фото- или видеосъемки днища автотранспортного средства.

2. Рабочая станция, обеспечивающая формирование итогового изображения днища автотранспортного средства и согласующая работу компонентов системы и дополнительного оборудования.

3. Сервер, как правило входящий в состав системы контроля и управления доступом и выполняющий функции формирования и хранения базы данных эталонных и ранее отсканированных изображений днищ автотранспортных средств, их регистрационных номеров и иных требуемых для идентификации параметров.

4. Автоматизированное рабочее место (АРМ) с установленным специализированным программным обеспечением (СПО), посредством которого производится просмотр итоговых изображений днища автотранспортного средства и управление системой.

Кроме того, в состав оборудования для досмотра днища автотранспортных средств могут входить системы:

- распознавания регистрационных номеров автотранспортных средств;
- получения изображения внешнего вида автотранспортного средства;
- регулирования движения автотранспортных средств (светосигнальные устройства – светофоры, устройства преграждающие управляемые, датчики въезда/выезда автотранспортного средства, а в некоторых системах – скорости его проезда);
- дистанционного контроля содержимого салона (возможность контроля наличия в салоне/кузове автотранспортного средства пассажиров или грузов) и др.

Модуль сканирования

Главным компонентом автоматизированной и автоматической системы досмотра днища является модуль сканирования, который может иметь стационарное исполнение, предназначенное для встраивания в поверхность дорожного полотна, либо мобильное исполнение, при котором модуль (рампа) закрепляется поверх дорожного полотна (рис. 2).

В общем случае в состав модуля входят видеокамера, оптическая система, система подсветки в видимом и инфракрасном спектре, ударопрочное защитное стекло, система подогрева, система очистки защитного стекла, влагозащищенный корпус.

Видеокамера

Основной элемент, формирующий изображение днища автотранспортного средства. Благодаря высокой скорости съемки обеспечивается возможность формирования изображения днища при движении автотранспортного средства, а высокое разрешение позволяет различать на итоговом изображении элементы размером до 0,5х0,5 мм.

В зависимости от конкретного исполнения видеокамеры ее фоточувствительный элемент может иметь различное соотношение сторон. При соотношении сторон, близком к 3:4, изображение формируется одним снимком и может быть откорректировано или дополнено несколькими другими снимками, получаемыми с одной или нескольких видеокамер.

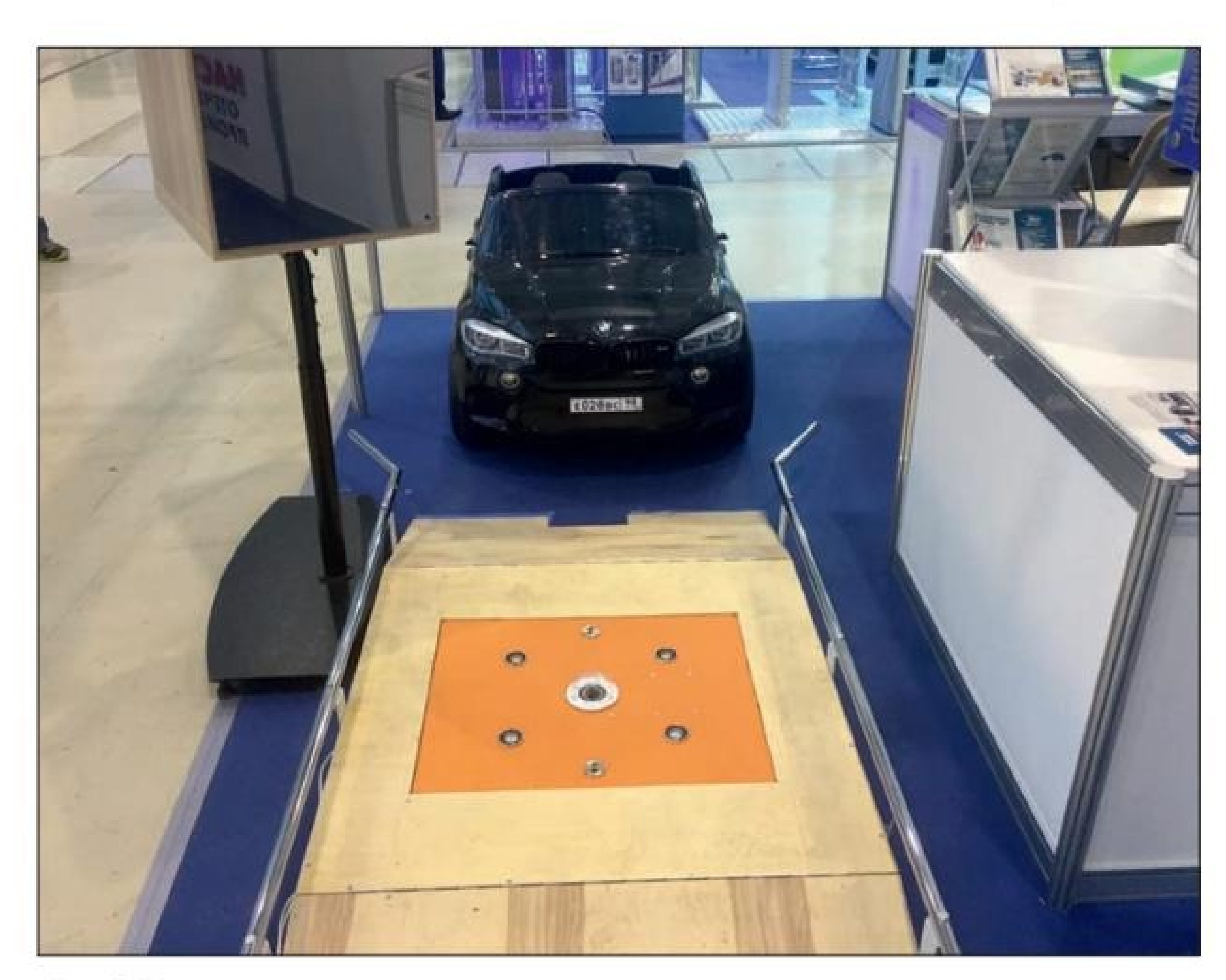


Рис. 2. Модуль сканирования

Учитывая тот факт, что системы досмотра днища автотранспортных средств направлены на предотвращение противоправных действий, в том числе террористического характера, защита от угрозы жизни и здоровью операторов, непосредственно задействованных в проведении досмотра, является немаловажной составляющей их эффективного и полноценного функционирования. Данная задача может быть решена либо с помощью применения специальных инженерно-технических решений, либо посредством удаления оператора АРМ за пределы потенциально опасной зоны

При линейном соотношении сторон фоточувствительного элемента видеокамеры изображение формируется построчно, по мере движения автотранспортного средства над модулем сканирования.

Оптическая система

Включает в себя набор оптических зеркал и призм, обеспечивающих точную фокусировку изображения днища проезжающего автотранспортного средства на фоточувствительном элементе видеокамеры. В ряде систем досмотра имеется возможность проведения съемки под углом к днищу, отличном от 90 град., что позволяет получить более широкий угол обзора.

Система подсветки

Обеспечивает необходимую интенсивность и направленность светового потока для корректной работы видеокамеры при высокоскоростной съемке движущегося объекта или съемке под углом, отличном от 90 град., в условиях недостаточной освещенности под днищем автотранспортного средства.

Защитное стекло

Минимизирует внесение оптических искажений и создает механическую прочность, обеспечивающую устойчивость к появлению царапин и разрушению при штатном режиме работы (очистка от абразивного загрязнения и др.) или при возникновении нештатных ситуаций (наезд колеса автотранспортного средства и др.).

Система подогрева

Необходима для обеспечения устойчивой работы модуля сканирования при отрицательных наружных температурах, повышенной влажности воздуха, образовании снежного покрова, обледенения или конденсата на защитном стекле.

Система очистки защитного стекла

Позволяет снизить влияние помех, вызванных загрязнением поверхности защитного стекла, при проведении досмотра днища и может быть выполнена как в составе модуля сканирования, так и являться отдельной вспомогательной системой. В зависимости от конкретной модели может обеспечивать механическое удаление загрязнения при помощи щеток или воздействия воздушных/водяных струй.

Корпус

Это несущий элемент модуля сканирования, механически объединяющий все составные части. Вне зависимости от исполнения модуля сканирования (стационарного или мобильного) корпус должен обеспечивать механическую прочность всей конструкции, выдерживать вес автотранспорта во время проезда, защищать от проникновения влаги, поддерживая работоспособное состояние внутренних элементов и всей системы в целом.

На какие характеристики обратить внимание?

Учитывая особенности условий эксплуатации, а также необходимость обеспечения работоспособности в большом числе климатических зон, следует выделить ряд наиболее важных технических характеристик, позволяющих провести всестороннюю оценку возможности применения указанных систем на конкретных объектах:

- степень автоматизации;
- конструктивное исполнение;
- номенклатура досматриваемых автотранспортных средств;
- удобство эксплуатации;
- уровень обеспечения безопасности обслуживающего персонала;
- климатическое исполнение;
- пропускная способность.

Наиболее целесообразно применять системы, рассчитанные на проведение автоматического досмотра днища автотранспортного средства.

Варианты исполнения

Конструктивное исполнение системы определяется способом размещения модуля сканирования относительно дорожного полотна:

- мобильное (позволяет оперативно осуществлять развертывание и свертывание системы);
- стационарное (требует проведения инженерно-технических подготовительных и установочных работ).

Стационарный способ размещения модуля сканирования имеет два варианта реализации:

1) "лежачий полицейский" (модуль располагается над дорожным полотном между рампами, по которым осуществляется проезд автотранспортных средств);

2) "уровень дорожного полотна" (модуль размещается в специально выполненном углублении, в плоскости дорожного полотна).

Способ размещения модуля сканирования в значительной степени определяет такие его конструктивные особенности, как степень защиты, обеспечиваемая его оболочкой, устойчивость к воздействию внешних неблагоприятных факторов и необходимость включения в состав конструкции дополнительного и вспомогательного оборудования (вспомогательных систем подогрева, охлаждения и обдува их защитных стекол).

Выбор систем досмотра по номенклатуре досматриваемых автотранспортных средств неоднозначен и определяется рядом факторов, наиболее важным из которых является пропускной режим автотранспортных средств, действующий на конкретном объекте, и возможный состав автопарка.

Тонкости правильной эксплуатации

Удобство эксплуатации системы досмотра – это субъективная комплексная оценка таких характеристик, как:

- степень автоматизации;
- наличие вспомогательного и дополнительного оборудования или систем, снижающих трудоемкость выполнения основных функций;
- эргономические показатели;
- дружественность интерфейса элементов управления системой досмотра;
- возможность управления системой при помощи АРМ, размещаемого в помещении, защищенном от воздействий внешних неблагоприятных факторов;
- трудоемкость развертывания и свертывания мобильных систем досмотра на объекте;
- степень ремонтопригодности и простота обслуживания элементов и модулей, входящих в состав системы.

Учитывая тот факт, что системы досмотра днища автотранспортных средств направлены на предотвращение противоправных действий, в том числе террористического характера, защита от угрозы жизни и здоровью операторов, непосредственно задействованных в проведении досмотра, является немаловажной составляющей их эффективного и полноценного функционирования. Данная задача может быть решена либо с помощью применения специальных инженерно-технических решений, либо посредством удаления оператора АРМ за пределы потенциально опасной зоны.

Климатическое исполнение системы определяет степень ее устойчивости к воздействиям климатических факторов. Особенности географического расположения России налагают специальные требования к оснащению систем досмотра днища автотранспортных средств дополнительным и вспомогательным оборудованием, например подсистемами кондиционирования, подогрева, очистки и т.д.

Пропускная способность характеризуется совокупностью ряда факторов, таких, как:

- максимальная скорость проезда автотранспортного средства, на которой возможно получение корректного изображение днища, государственных регистрационных номеров и содержимого салона или кабины;
- степень автоматизации;
- время, необходимое для обработки изображения досматриваемого транспортного средства.

Скорость проезда должна коррелироваться со временем, необходимым для обработки изображения днища и принятия решения о допуске. Высокое значение скорости проезда неприемлемо для организации пропускного режима с применением локально расположенных точек доступа, так как снижает его надежность.

Таким образом, правильно выбранная и эксплуатируемая система досмотра днища автотранспортных средств является необходимым и надежным компонентом для обеспечения безопасности функционирования охраняемых объектов и проведения массовых мероприятий. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Александр Дремин
Генеральный директор
компании BIOSMART

Отечественная или зарубежная?

Как выбрать биометрическую систему и не пожалеть?

Биометрические технологии блестяще зарекомендовали себя в период пандемии: в 2020 г. во многих офисах и на производственных площадках появились биометрические комплексы для идентификации, дистанционного измерения температуры и даже алкотестирования. За несколько месяцев биометрия вошла в моду и, как это часто бывает с популярными решениями, мгновенно обросла мифами и обрела репутацию панацеи против любых "недугов" в области управления персоналом и учета рабочего времени. Однако, когда заказчики массово бросились закупать и устанавливать первые попавшиеся биометрические комплексы, результаты внедрений оказались... разочаровывающими.
О том, почему это происходит, как избежать чужих ошибок и выбрать подходящее биометрическое решение, рассказывает CEO BIOSMART Александр Дремин, руководитель одного из ведущих российских вендоров биометрии, эксперт-практик с 15-летним стажем

Любой проект по внедрению биометрии состоит из двух этапов:
- глубинного анализа задачи и подбора подходящего технологического решения;
- внедрения и эксплуатации.

Ошибка на каждом из этапов может стать фатальной. Рассказываем, как лучше действовать и на что обратить внимание.

Разберитесь в задаче и сформируйте четкое ТЗ для вендора

Возьмите паузу и проанализируйте прецедент

Мелкие операционные потери или редкие случаи нерационального расходования средств в бизнесе неизбежны и, как правило, уже заложены в цену выпускаемого товара или услуги. Любое предприятие – это живой, растущий организм, и никто не требует от него точности швейцарских часов.

Однако зачастую собственник компании даже не догадывается об истинных объемах денег, утекающих сквозь щели в системе безопасности... ровно до того момента, пока одна из таких щелей не будет обнаружена. Это может быть "узкое место" в контроле за персоналом, аутстафферами или посетителями; "дыра" в цифровой безопасности или карточная СКУД, "электронные ключи" от которой давным-давно есть у всех сотрудников, их жен и домашних питомцев.

В такие моменты идея о внедрении биометрии кажется максимально привлекательной: хочется как можно скорее покончить с воровством или обманом, наказать мошенников и заблокировать найденную точку потери средств... И, как показывает наш опыт, именно в такие моменты ни в коем случае не следует поддаваться порыву и принимать спонтанные решения.

При возникновении прецедента такого рода прежде всего постарайтесь досконально разобраться в ситуации. Убедитесь, что вам точно известны ответы на главные вопросы: как именно удалось нечистым на руку сотрудникам провернуть преступную схему? кто мог участвовать в ней? какие ошибки, допущенные при проектировании системы безопасности, сделали это возможным?



Современные биометрические системы обладают широким функционалом, позволяющим решать множество разных задач, от учета рабочего времени и мониторинга действий персонала до контроля сотрудников на удаленке и сотрудников с выездным характером работы.
Главное – подобрать решение, которое подойдет именно вам, и надежного вендора, которому вы доверяете и который станет вашим проводником в мире биометрии

Изучите кейс максимально глубоко – только так вы сможете управлять рисками и предотвращать новые угрозы на системном уровне. Просто поставить камеру в том месте, где кто-то что-то однажды украл, недостаточно. Нужно создать комплексную систему, которая сделает кражу невозможной.

Тщательно изучив кейс, вы поймете, чего на самом деле хотели бы от биометрии. Теперь пора описать ваши ожидания в формате ТЗ.

Четко опишите задачу, особенности проекта и желаемый результат

Прежде чем выбирать вендора и технологическое решение, сформируйте как можно более полное техническое задание, в котором будут упомянуты все значимые детали, нюансы и подробности.

В базовом ТЗ обязательно должны быть отражены следующие моменты:
- собственно ваши ожидания от биометрической системы;
- задачи, которые она должна решать;
- охранные и ERP-системы, уже установленные на предприятии;
- структура объекта, сколько в нем точек прохода (в том числе уличных), имеющиеся периметры и уровни доступа;
- количество людей, работающих на предприятии;

- условия работы персонала (производство, офис, уличные объект и пр.);
- графики работы персонала;
- "узкие места" в контроле за персоналом;
- бизнес-процессы, в которых участвуют аутстафферы, способы контроля их работы.

Современные биометрические системы обладают широким функционалом, позволяющим решать множество разных задач, от учета рабочего времени и мониторинга действий персонала до контроля сотрудников на удаленке и сотрудников с выездным характером работы.

Главное – подобрать решение, которое подойдет именно вам, и надежного вендора, которому вы доверяете и который станет вашим проводником в мире биометрии.

Прогнозы развития отечественного рынка биометрии

В 2020 г. по инициативе Минпромторга России был принят ряд нормативных документов, в частности по 30%-ному преимуществу в цене для российского оборудования, запрету на включение в документацию дополнительных характеристик, квотированию закупок отечественной радиоэлектронной промышленности, налоговым льготам для ИТ-разработчиков.

В 2021 г. представители отраслевого сообщества подали в профильные комитеты Совета Федерации еще ряд предложений, многие из которых, по нашим прогнозам, могут быть приняты уже в перспективе ближайших месяцев.

В их числе:

- **создание единого центра аттестации промышленной продукции, консолидирующего техническую документацию на все виды аппаратуры из Единого реестра российской электронной продукции;**
- **снижение налога на прибыль и налога на добавленную стоимость для российских разработчиков электроники и ПО;**
- **субсидии до 50% стоимости на покупку и пилотирование проектов с использованием отечественной электроники;**
- **запрет на использование иностранных продуктов с проприетарными решениями зарубежных правообладателей на объектах критической информационной инфраструктуры и полный переход этих объектов на российские программно-аппаратные решения к 2025 г.**

Планируйте внедрение биометрии как стратегический проект с учетом прогнозов по рынку

Биометрическая СКУД – одна из базовых систем предприятия. Она интегрирована с охранными комплексами, системами начисления заработной платы и различными кастомными программными комплексами. Как следствие, она должна сохранять актуальность хотя бы в горизонте пяти лет, а по прошествии этого времени любые морально устаревшие компоненты должны легко заменяться более передовыми аналогами. Причем расходы на плановое обновление системы должны быть на несколько порядков меньше, чем ее капитальная реорганизация или замена.

Таким образом, внедрение СКУД – это стратегическое решение. Поэтому при выборе технологического решения (и вендора) нужно учитывать те тренды, которые мы наблюдаем сейчас, и предупредить те трудности, которые могут возникнуть в ходе эксплуатации системы.

Убедитесь в доступности вендора

Биометрическая СКУД – высокотехнологичный и сложный продукт, при использовании которого у пользователей возникают тысячи вопросов. Иногда заказчику нужна помощь в настройке или консультация по неочевидным функциям системы. Иногда уже в процессе эксплуатации заказчик понимает, что у него есть потребность в "подгонке" системы и внедрении кастомного решения.

В каждый из этих моментов вендор должен быть рядом и готов помочь. На практике мы убедились, что обеспечить достаточный объем поддержки может только отечественный разработчик. Вероятность, что он оперативно рассмотрит любой вопрос и предложит оптимальное решение, намного выше, чем при обращении к какому-нибудь зарубежному вендору... который, признаемся честно, вряд ли даже будет рассматривать такого рода запросы из-за рубежа.

Продумайте возможности интеграции

Современная СКУД должна органично встроиться в другие инженерные сети предприятия и работать в одной команде с охранными и ERP-системами, установленными в разное время и разными вендорами. Не только сегодня, но и через 5–10 лет, несмотря на стремительное развитие технологий.

Качественная СКУД поддерживает интеграцию как на аппаратном, так и на программном уровне.

В настоящее время в СКУД активно применяются два типа аппаратной интеграции – Wiegand и OSDP. Протокол Wiegand более популярен и кажется вполне подходящим для решения большинства задач. Но мы рекомендуем присмотреться к протоколу OSDP. Он разработан намного позже, чем Wiegand, лучше защищен от помех, имеет возможность шифрования данных и может работать на расстоянии до 300 м от контроллера.

Программная интеграция реализуется с помощью SDK и REST API. REST API предпочтительнее, так как при использовании этого метода программирование сведено к минимуму, а все команды со сторонними библиотеками описываются специальными языками JSON или XML.

И разумеется, в СКУД должна быть предусмотрена интеграция в сторонние системы, включая системы видеонаблюдения и ОПС, а также интеграция с исполнительными устройствами (алкотестерами, датчиками температуры, тревожными кнопками и т.д.).

Спрогнозируйте рентабельность в рамках всего жизненного цикла проекта

Чтобы спланировать экономическую состоятельность проекта в горизонте хотя бы пяти лет, нужно иметь представление о существующих трендах. В биометрической отрасли сегодня их два – ставка на нейросетевые алгоритмы и ставка на импортозамещение. И если с первым все более-менее понятно – скорость, безопасность, эффективность нейросетей очевидна каждому пользователю, то второй заметен пока только специалистам.

Как активные участники рынка, мы видим, что российские законодатели активно взялись за совершенствование нормативно-правовой базы, регулирующей производство электроники и программного обеспечения. Данная отрасль считается системообразующей и стратегически значимой, при этом на сегодняшний день уровень российских разработок в области электроники не только не уступает, а даже превосходит уровень зарубежных аналогов. А уровень безопасности российского ПО намного выше, чем уровень безопасности ПО от неизвестных западных или восточных поставщиков.

Как следствие, в органах государственной власти горячо обсуждается целый ряд законопроектов в области поддержки отечественного производителя электроники и создания заградительных мер для импортеров. В общем, в центре внимания вопросы импортозамещения и обеспечения технологической независимости в этой сфере.

Даже если не все из указанных законопроектов и предложений отраслевого сообщества будут приняты, в ближайшие годы тренд на потребление отечественной продукции усилится.

Заказчики, выбирающие отечественные решения, будут получать поддержку со стороны государства как в форме прямых субсидий на покупку и пилотирование российских разработок, так и в форме налоговых послаблений. Импортная электроника, в свою очередь, будет облагаться таможенными пошлинами и особенно тщательно проверяться на соответствие национальным стандартам безопасности. Проверку пройдут не все.

Мы прогнозируем, что уже в перспективе ближайших двух лет разница в стоимости отечественных и зарубежных решений будет заметна любому потребителю. Часть зарубежных решений вообще больше не попадет на российский рынок как не соответствующая стандартам.

Поэтому всем, кто планировал приобретать биометрическую систему от иностранного поставщика, мы настоятельно рекомендуем задуматься и еще раз оценить возможные риски проекта. Биометрия останется с вами надолго. Стоит ли сегодняшняя экономия повышенных расходов в будущем? ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

АДИС: скорость, анализ, результат

Основная задача автоматизированной дактилоскопической информационной системы (АДИС, в зарубежных источниках AFIS) – автоматизация процесса установления личности по следам рук (отпечаткам ладоней и/или отпечаткам пальцев рук), а также ведение автоматизированного криминалистического учета и, соответственно, внедрение автоматизированных дактилоскопических идентификационных систем. Применение современных АДИС – одно из необходимых условий для организации высокоэффективной работы правоохранительных органов



Данила Николаев
Директор Некоммерческого партнерства "Русское биометрическое общество", председатель ТК 098 "Биометрия и биомониторинг"



Василий Мамаев
Заместитель директора Некоммерческого партнерства "Русское биометрическое общество", заместитель председателя ТК 098 "Биометрия и биомониторинг"

АДИС позволяет решать множество задач и беспечивает:

- сокращение трудозатрат и повышение эффективности раскрытия и расследования преступлений за счет более точной и своевременной информации, предоставляемой оперативным службам;
- возможность установления личности как живых лиц, так и неопознанных трупов по нескольким отпечаткам пальцев рук, небольшому фрагменту только одного отпечатка (даже при значительных изменениях);
- автоматическую проверку дактилоскопической информации по базе данных АДИС при постановке на дактилоскопический учет и при исполнении оперативных запросов;
- ускорение обработки дактилоскопической информации при постановке на учет и уменьшение времени ответа на запросы;
- повышение результативности дактилоскопических учетов;
- улучшение качества поступающей дактилоскопической информации за счет внедрения оптоэлектронных устройств бескраскового дактилоскопирования – "живых" сканеров;
- возможность объединения учетов в единую автоматизированную систему;
- реализацию межрегионального взаимодействия автоматизированных дактилоскопических учетов.

При использовании АДИС следы пальцев рук и дактокарты сканируются, кодируются на электронные носители информации и проверяются в режимах:

- следы – дактокарты;
- дактокарты – следы;
- следы – следы;
- дактокарты – дактокарты.

Основные производители

По прогнозам экспертов, глобальные доходы[1] от рынка АДИС к 2025 г. вырастут до 12,46 млрд долларов с показателем CAGR 18,4%, а согласно исследованию Grand View, передовые системы безопасности будут все более востребованы в различных отраслях промышленности. Растущее внедрение мобильных платежей и спрос на интегрированные решения АДИС также будут стимулировать рост.

Ожидается, что значительная доля рынка будет приходиться на государственный сегмент и сферу программного обеспечения. Северная Америка станет крупнейшим региональным рынком на протяжении всего прогнозируемого периода с долей в 4,05 млрд долларов к 2025 г.

Среди ключевых игроков рынка были определены Gemalto, NEC Corporation, Crossmatch (ныне принадлежащая HID), IDEMIA, DERMALOG, Suprema, Fujitsu, Sonda Technologies, HID Global, Papillon Systems, East Shore Technologies и AFIX Technologies.

Как мы видим, Россия на международном рынке АДИС представлена двумя компаниями: "Папилон" (Papillon Systems) и "Сонда" (Sonda Technologies).

Структура АДИС

АДИС – это модульная система, масштабируемая от небольшой локальной базы данных дактилокарт и следов на типовом ПК или ноутбуке до гигантских территориально распределенных комплексов национального уровня, построенных в соответствии с концепцией "центральный комплекс АДИС + сеть периферийных станций"[2].

В основу работы АДИС положена архитектура "клиент – сервер", поддерживающая независимое обращение рабочих станций к обслуживающему запросы серверу. Процесс поисков организован по технологии распределенных вычислений.

В крупных комплексах серверные функции – ввод и хранение данных, поиски, связь и коммуникации распределены между отдельными подсистемами:

- сервером и вычислителями АДИС;
- подсистемой хранения данных;
- подсистемой связи и коммуникаций;
- сервером и вычислителями оперативных проверок.

В комплексах с небольшими БД серверные функции обеспечиваются ресурсами единого серверного блока или распределяются между рабочими станциями.

Подсистема хранения данных состоит из дисковых накопителей и сервера, предназначенного для выделения текстовой части БД АДИС в отдельную базу данных, открытую для взаимодействия с внешними SQL-системами через веб-браузеры.

Требуемый состав оборудования определяется размером базы данных и планируемой плотностью потоков дактилоскопической информации и запросов на проверки, поступающих от рабочих станций, которые входят в состав комплекса, и с периферийных станций в режиме удаленного доступа.

Ключевые параметры

Функционально АДИС должна обеспечивать:

- ввод и хранение в БД дактилокарт, фотоизображений лиц и особых примет, словесного описания людей;
- ввод и хранение в БД следов пальцев рук и ладоней, изъятых с мест преступлений;
- проведение автоматических поисков типов "карта – карта", "карта – след", "след – карта", "след – след";
- поиск по словесному описанию;
- проведение поисков и идентификацию следов и отпечатков ладоней;
- автоматизированное определение дактилоформулы;
- автоматизированный дактилоучет (проведение многообразных выборок, сортировка списков БД, удаление и редактирование записей и т.д.);

[1] https://www.biometricupdate.com/201905/biometrics-research-briefs-afis-identity-verification-europe-and-voice-biometrics
[2] https://www.papillon.ru/rus/22/

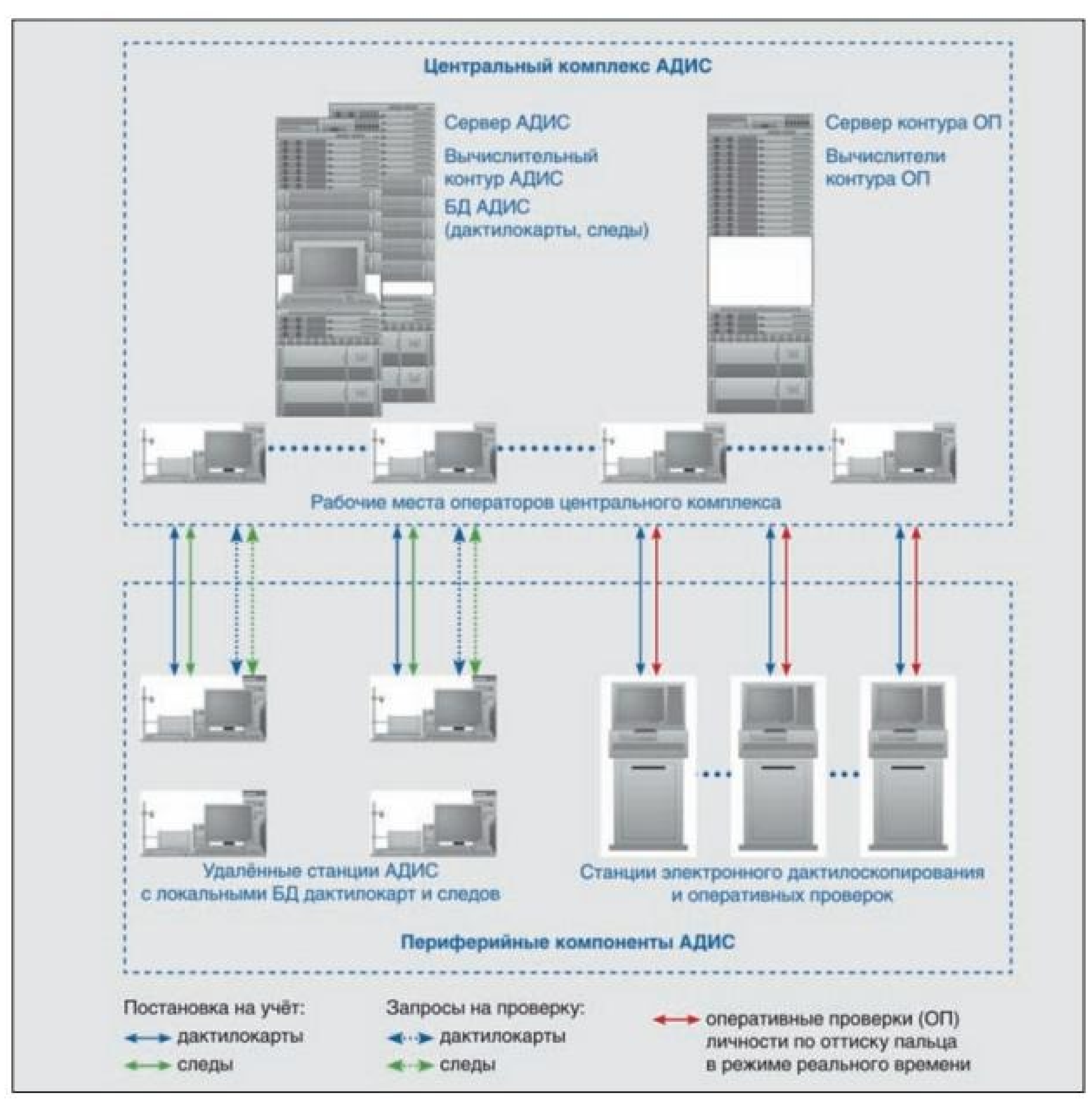


Рис. 1. Пример построения типового территориально распределенного комплекса АДИС

- вывод графических изображений (дактилокарт, фотоизображений, следов) на монитор и на принтер, печать документов, списков, справок, статистической информации;
- удаленный ввод дактилоскопической информации, удаленный доступ к центральной БД, построение распределенных систем;
- соответствие основным требованиям по многоуровневому разграничению доступа и закрытию информации, передаваемой по каналам связи и хранящейся в базе данных;
- взаимодействие с другими видами автоматизированных учетов;
- импорт/экспорт дактилокарт и следов в формате Интерпола, ФБР, МВД России, ГОСТ Р и ИСО/МЭК.

Без выполнения вышеперечисленных функций АДИС любого производителя будет неспособна выполнять свою основную задачу – максимально облегчить работу сотрудникам правоохранительных органов при определении личности гражданина.

Основными техническими параметрами АДИС являются:

- максимально возможный размер базы данных, с которым может работать АДИС;
- скорость обработки в режимах "следы – дактилокарты", "дактилокарты – следы", "следы – следы", "дактилокарты – дактилокарты".
- точность определения результата, выраженная в величине ошибок распознавания.

Скорость обработки указывается как скорость идентификации в выбранную единицу времени.

Количество записей, содержащихся в базах по всему миру, растет с каждым днем, поскольку в них систематически добавляются новые сведения. В ФБР находится одна из самых больших баз дактилокарт, содержащая более 60 млн записей. Помимо получения собственных записей, более 18 тыс. учреждений ежедневно в электронной форме отправляют в базу ФБР отпечатки, изъятые с мест преступлений. Поэтому размер базы увеличивается каждый день более чем на 10 тыс. изображений, и 96% из них являются электронными. Интерпол – крупнейшая в мире полицейская организация – имеет базу данных отпечатков пальцев в 104 тыс. записей[3] (данные 2013 г.).

Примеры внедрения

Развитие АДИС в мире привело к тому, что основные компании добиваются значительных результатов. Так, компания DERMALOG[4] благодаря биометрическому высокоскоростному распознаванию может сопоставить отпечатки пальцев всего населения мира в течение нескольких секунд. Тестирование в соответствии с международным стандартом ISO/IEC 19795-1 проводилось компанией SGS-TÜV Saar, которая и установила данный рекорд скорости. Система сравнивала около 3,6 млрд пальцев в секунду и точно определяла возможные совпадения.

Фирма Gemalto[5] с помощью технологии Field-Programmable Gate Array (FPGA), изначально разработанной для приложений со сверхнизкими задержками в средах высокопроизводительных вычислений (HPC) в финансовых и научных индустриях, сообщает о возможности многократной обработки сотен миллионов записей биометрической базы данных в течение 1–2 секунд. К сожалению, для данных тестов не приводятся параметры качества сравнения.

Комплексы АДИС российских компаний[6, 7] функционируют не только в России (МВД, ФСБ, ФСКН, ФМС, ФТС), но и в Албании, Бангладеш, Боснии и Герцеговине, Вьетнаме, Индии, Кубе, Нигерии, Казахстане, Монголии, Сербии, Таджикистане, Туркмении, Турции, Узбекистане, Черногории, Украине, Латвии, Молдавии, Киргизии, Сирии, Уругвае, Гватемале, Китае и др.

Среди крупных проектов можно отметить АДИС-МВД (50 млн дактилокарт, 250 тыс. следов) и системы в:

- Турции (35 млн дактилокарт, 1,5 млн следов);
- Узбекистане (20 млн дактилокарт);
- Индии (10 млн дактилокарт, 500 тыс. следов).

Проблемы эксплуатации

Стабильность и устойчивость поисковых характеристик АДИС[8] зависят от целого ряда факторов:

- способности системы одинаково надежно работать с дактилоскопическими изображениями различного качества;
- способа описания папиллярного узора и избирательности алгоритмов сравнения;
- совершенства алгоритмов распознавания и кодирования папиллярного узора;
- степени автоматизации всех этапов обработки дактилокарт и следов.

Данные по распределению статистики следов разного качества приведены на рис. 2.

10 критериев эффективности

Для предварительной оценки эффективности различных АДИС можно использовать следующие критерии[9]:

1. Полнота реализованного в системе математического способа описания папиллярного узора.
2. Точность автоматического кодера, которую можно косвенно оценить по степени участия оператора в процессе кодирования.
3. Быстродействие системы.
4. Размер выдаваемых рекомендательных списков.
5. Положение "родного" кандидата в рекомендательных списках с учетом выбранного ранга.
6. Способность системы работать с реальными массивами дактилокарт и следов без предварительного отбора их по качеству.

[3] Холевчук А.Г. Автоматизированная система идентификации отпечатков пальцев: опыт США // Вестник криминалистики. 2019. № 1 (69). С. 32–42.
[4] https://www.dermalog.com/news/article/fingerprint-matching-world-record/
[5] https://safetyarea.ru/news/tekhnologiya-gemalto-pomogaet-povysit-biometricheskuyu-proizvoditelnost/
[6] https://www.papillon.ru/rus/20/
[7] http://sonda.ru/product/afis/afis_sonda.html
[8] Практические вопросы выбора эффективной автоматизированной дактилоскопической идентификационной системы (АДИС). Зайцев П.А., генеральный директор ЗАО "ПАПИЛОН", г. Миасс, Челябинская обл.
[9] https://www.papillon.ru/rus/21/

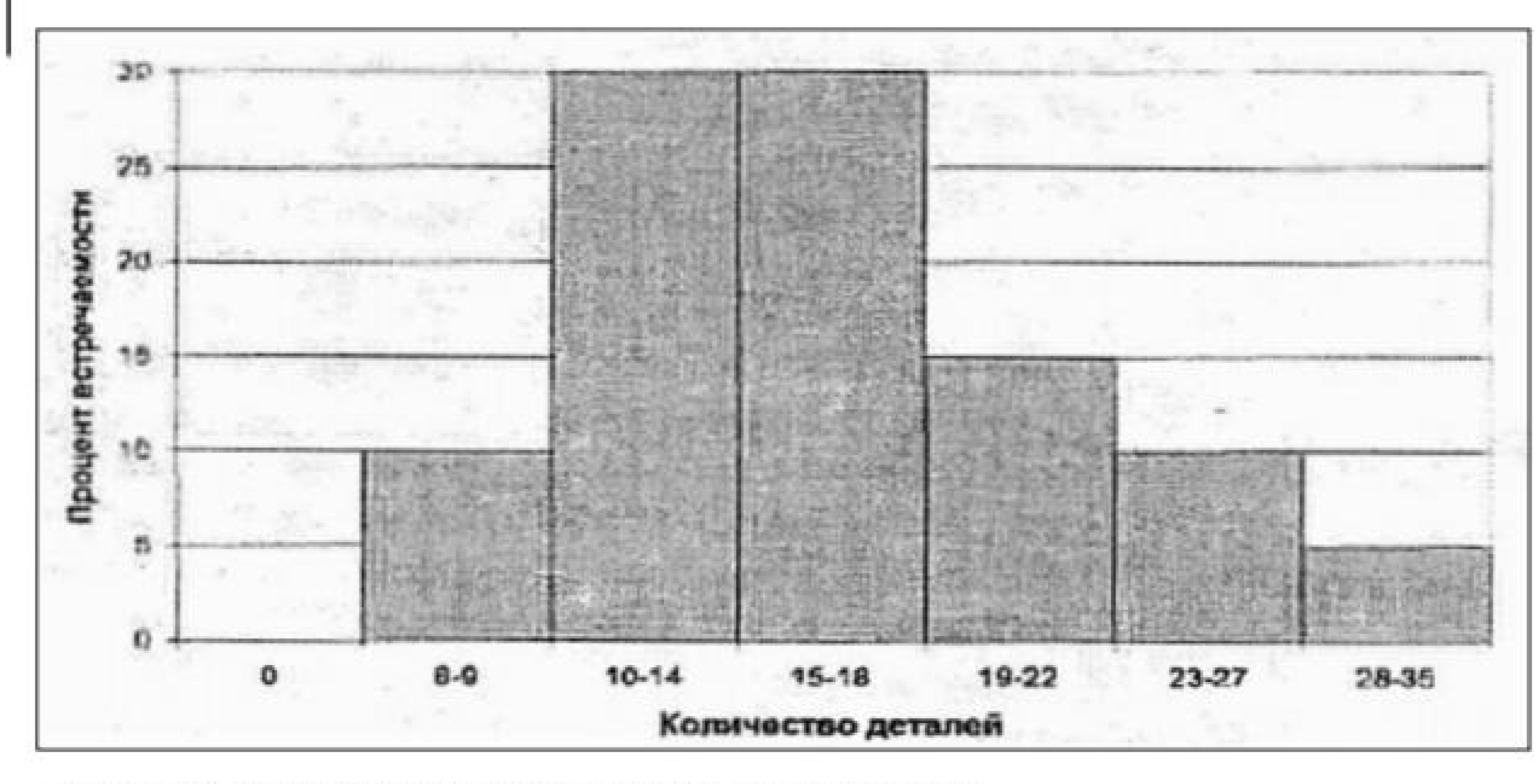


Рис. 2. Статистика встречаемости следов разного качества

7. Способность системы работать с разномасштабными изображениями.
8. Способность системы работать со следами и отпечатками ладоней.

9. Наличие современных высококачественных технологий ввода (бескрасковое дактилоскопирование, видеоввод).

10. Практическое распространение системы и масштабность реализованных с применением данной АДИС проектов (объемы БД дактилокарт и следов).
Объективное сравнение количественных показателей надежности и точности различных АДИС возможно лишь по результатам полномасштабных сравнительных испытаний. Тестирование должно проводиться на реальных массивах дактилокарт и следов по тщательно проработанным методикам, обеспечивающим абсолютно равные условия для всех испытуемых систем.

Проведение испытаний биометрических систем должно проводиться на основе национальных стандартов ГОСТ Р ИСО/МЭК 19795-1–2007, ГОСТ Р 58292–2018 (ИСО/МЭК 19795-2:2007), ГОСТ Р ИСО/МЭК ТО 19795-3–2009, ГОСТ Р ИСО/МЭК 19795-4–2011, ГОСТ Р ИСО/МЭК 19795-6–2015 и др.

В следующей статье рассмотрим сравнение различных алгоритмов распознавания отпечатков пальцев на основе материалов NIST. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Денис Плюшкин
Начальник отдела технических средств охраны службы защиты информации и систем охраны Департамента обеспечения безопасности и предотвращения потерь компании "Спортмастер Россия"

Внедрение системы распознавания лиц с измерением температуры на проходной в бизнес-центре

Главная задача системы управления доступом в современном бизнес-центре – это обеспечение контрольно-пропускного режима как фундаментальной основы безопасности офисного пространства. Однако текущий уровень развития технологий и пандемия 2020 г. предъявляют дополнительные требования к базовой функциональности систем управления доступом



Входная группа офиса бизнес-центра, где размещается ООО "Спортмастер"

СКУД в бизнес-центре должны обладать такими характеристиками, как:
- современный дизайн;
- большая пропускная способность;
- надежность;
- комбинации традиционных, мобильных и биометрических идентификаторов;
- бесконтактный тепловизионный автоматический контроль температуры;
- масштабируемость;
- модульное построение, простая модернизация;
- простая интеграция с кадровыми системами и системами учета рабочего времени.

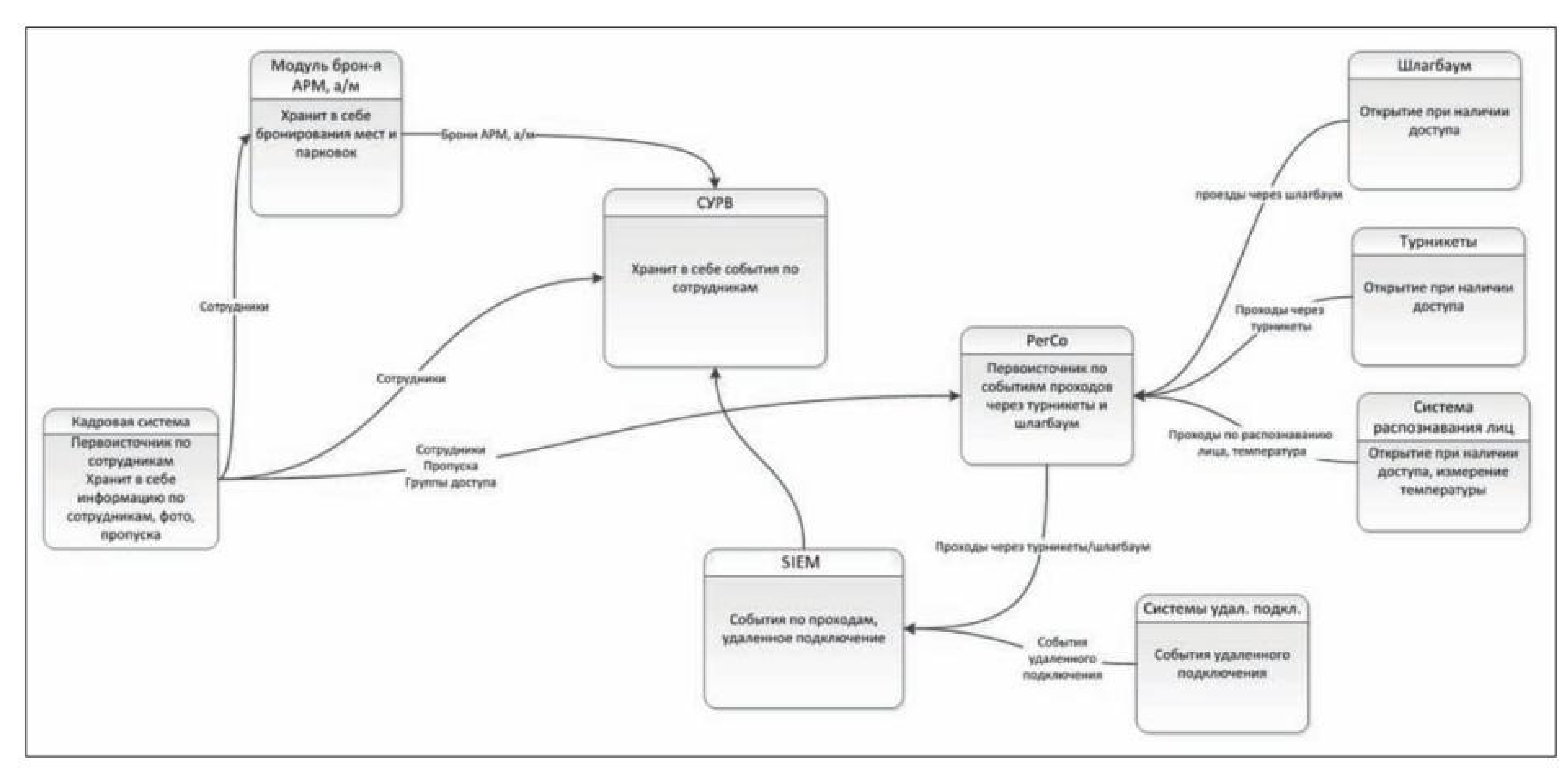
Поставленные цели

Перед руководством бизнес-центра на 4 тыс. сотрудников стояли конкретные задачи:
- бесконтактное измерение температуры на входе;
- проход по распознаванию лиц с сохранением существующей СКУД и выданных карт доступа;
- современный дизайн.

Внедрение терминалов распознавания лиц с функцией тепловизионного контроля обеспечивало выполнение всех вышеперечисленных требований при определенных условиях:
1. Четко сформулированные задачи внедрения и критерии их приемки.
2. Понимание необходимости и глубины интеграции в смежные информационные системы компании.
3. Наличие достаточной компетенции в системах контроля доступа и ИТ-технологиях как со стороны заказчика, так и со стороны подрядчика-интегратора.
4. Проведение подготовительных мероприятий с кадровыми подразделениями по сбору биометрических данных и согласий на их обработку.

Первая попытка внедрения

После пилотирования семи систем от производителей – лидеров на рынке программного обеспечения для распознавания лиц было принято решение использовать терминалы распознавания только для трансляции видеопотока на сервер с установленным программным обеспечением. Управляющие сигналы далее передаются в систему управления



Пример схемы потоков данных современной системы контроля доступа

доступом с параллельной верификацией по температурным параметрам, получаемым с терминала отдельным промежуточным сервером и передаваемым также в систему управления доступом.

Уже предварительное опытное тестирование показало узкие места и проблемы данного подхода:

- структурная сложность системы и трудоемкость общего объема интеграций;
- недостаточный уровень быстродействия и надежности "железа" терминалов на момент внедрения;
- проблемы при распознавании лиц в масках любого типа;
- низкая точность бесконтактного измерения температуры.

В период тестирования на рынке появились новые продукты, которые позволили решить все вышеозвученные проблемы, но при изменении подхода к построению системы.

Вторая итерация

Лидеры рынка терминалов распознавания лиц (ZKTeco, RusGuard) разработали новые модели терминалов, лишенные недостатков первых моделей, которые позволяют получать отличные результаты распознавания лиц в масках непосредственно на терминале, а также добавлять при необходимости верификацию по температуре и наличию маски. Модель модернизации системы контроля доступа была пересмотрена в сторону упрощения и повышения надежности:

- обработка видеопотока на терминале распознавания лиц встроенным программным обеспечением, передача в систему контроля доступа только идентификатора в случае успешного распознавания;
- обработка информации о температуре на терминале, передача в систему контроля доступа бинарного значения валидации температуры;
- фиксация всех значений измеренной температуры независимо от распознавания и передача на сервер в фоновом режиме.

Простота базовой интеграции

Встроенный функционал базовой интеграции терминалов RusGuard с большинством систем контроля доступа на российском рынке позволяет запускать систему буквально в день установки. У предлагаемого программного обеспечения ограниченный функционал, но благодаря ему терминалы полностью готовы к работе в составе общей системы контроля доступа буквально в считанные часы. Это позволяет быстро понять и оценить применимость системы, качество и быстродействие работы терминала, а дальнейшую интеграцию можно прорабатывать на любом уровне через открытый API.

Реализованное итоговое решение

На базе терминалов RusGuard и существующей системы контроля доступа бизнес-центра PERCo реализована новая гибридная система контроля доступа, обладающая следующими характеристиками:

- бесконтактное измерение температуры – 100%-ное исключение контакта с персоналом охраны, блокирование доступа при превышении температуры;
- увеличение скорости измерения температуры и общей пропускной способности на вход в часы пик;
- распознавание лиц в надетой защитной маске;
- оповещение/запрет на вход без медицинской маски;
- не распознанные по лицу сотрудники и гости имеют возможность прохода по карте только с измерением температуры;
- современный минималистичный дизайн;
- удобство использования лица в качестве идентификатора, так как отсутствует необходимость предоставлять физический носитель (пропуск, брелок, NFC);
- сохранение существующей системы контроля доступа и выданных карт доступа;
- автоматизированный контроль приема и увольнения персонала за счет интеграции с кадровой системой;
- автоматизация управления уровнями доступа;
- передача функционала фотографирования в кадровые подразделения;
- реализация системы доступа к предварительно забронированным рабочим местам в офисе и на парковке;
- интеграция в систему учета рабочего времени более высокого уровня с помощью данных авторизации из большинства информационных систем компании для построения полной модели присутствия персонала на рабочем месте.

Полнота интеграции

Получение качественного конечного продукта с полной автоматизацией поддержки сопровождения возможно только при правильном проектировании архитектуры системы и ее интеграционных взаимосвязей.

Ниже перечислены основные информационные системы, которые вместе с системой контроля доступа организовали информационное пространство, позволяющее полноценно и без рутинной работы специалистов безопасности контролировать потоки персонала и гостей в бизнес-центре:

- система контроля и управления доступом;
- кадровая система;
- модуль бронирования АРМ и парковки автомобиля;
- система учета рабочего времени;
- SIEM с логированием удаленных подключений и авторизаций в ИС. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА РЕДАКТОРА

Безопасность или маркетинг?



Чтобы успешно заниматься торговлей, надо хорошо понимать покупателей. Эту истину знает каждый удачливый продавец, кто трудится в розничной торговле. Именно в этой области система видеонаблюдения более востребована в качестве ключевого инструмента исследования поведения покупателей. Безопасность же часто становится здесь второстепенной задачей. В этом нет ничего удивительного, так как, к примеру, выкладка товара в нужном месте и в нужном виде может принести гораздо больший доход владельцу магазина, нежели экономия от пойманного воришки.

Неудивительно, что именно розничная торговля является локомотивом в создании самых разнообразных модулей видеоаналитики. Иная программа может "отбиться" за пару месяцев, принося в дальнейшем чистую прибыль. Более того, в условиях жесткой конкуренции отказ от видеоанализа не позволит "выжать максимум" из имеющейся торговой площадки, что чревато потерей позиций в бизнесе.

Программные модули видеоаналитики прошли долгий путь от незатейливых детекторов движения до автоматизированных комплексов управления торговыми залами. Теперь тепловые карты помогают администраторам понять, какими маршрутами удобно двигаться покупателям, у каких витрин они задерживаются, а какие проскакивают, не останавливаясь. Детектор очереди позволяет добиться оптимального соотношения между удобством покупателей и количеством обслуживающего персонала, а интеграция видеонаблюдения с кассовым аппаратом способствует своевременному выявлению сговора покупателя с кассиром. Счетчик покупателей, вкупе с определением их пола и возраста, дает маркетологу бесценную статистику, позволяющую четко выделить целевые группы клиентов.

На долю безопасности остается система распознавания лиц в комплекте с базой данных злоумышленников. Такая система может серьезно снизить воровство, или, по-модному, шоплифтинг, а также сразу обращать внимание персонала на проблемных покупателей, однако требует постоянного обновления базы данных. При этом сама по себе база является подборкой персональных данных, хранение и использование которых может быть расценено как нарушение законодательства.

Михаил Арсентьев
Редактор раздела "Видеонаблюдение", коммерческий директор ООО "Артсек"

Задачи видеонаблюдения в ритейле расширяются

Мнения экспертов

Системы видеонаблюдения и видеоаналитики как в отдельных магазинах, так и в крупных торговых центрах не только позволяют решать задачи безопасности, но и выступают эффективным маркетинговым инструментом, способствуя росту прибыли. Эксперты компаний "Делетрон", КРОК и "Аккорд-СБ" проанализировали влияние видеонаблюдения на сокращение потерь, оценили эффективность конкретных модулей видеоаналитики и назвали оптимальные технологии для внедрения и интеграции в ритейле



Евгений Золотарев
Директор ООО "Делетрон"



Артем Романов
Руководитель направления систем безопасности ИТ-компании КРОК

Назовите основные задачи видеонаблюдения в ритейле

Евгений Золотарев, "Делетрон"

С точки зрения бизнеса и безопасности все смещается в сторону предиктивного анализа. Со стороны бизнеса это отслеживание действий покупателя: анализируются его предпочтения, демонстрируется персонализированная реклама на видеопанелях, составляются тепловые карты для оптимизации в торговом зале и контролируются очереди. Другое направление – это контроль товаров: их наличие в достаточном количестве на прилавках и качество продукции, в том числе овощей и фруктов, которое является актуальной проблемой для ритейлеров на сегодня.

Со стороны безопасности это распознавание лиц, ведение черных списков шоплифтеров, видеоаналитика подозрительной активности посетителей магазина еще до момента совершения кражи. Основные задачи видеонаблюдения на сегодня – это видеоаналитика и прогнозирование на основе AI для бизнеса и безопасности в одном техническом решении.

Артем Романов, КРОК

Если смотреть на видеонаблюдение как на систему обеспечения безопасности, то за 15 лет работы с заказчиками розничного сектора основные задачи остались прежними: отображать информацию о происходящем онлайн и вести запись, чтобы увидеть нарушение или провести расследование инцидента. Все-таки видеонаблюдение – это в первую очередь наблюдение, даже если оно может вестись из практически любой точки планеты. Контроль процесса оплаты и операций с наличными деньгами на кассах – основная задача с точки зрения защиты от попыток мошенничества.

Если взглянуть шире и учитывать модули видеоаналитики, то список задач сильно расширяется. Однако не все, что предлагает аналитика, я бы отнес к основным задачам, да и в целом они сильно разнятся в зависимости от типа точки ритейла. Подсчет уникальных посетителей, предупреждение о потенциальном воре, тепловые карты – для разных магазинов эти задачи тоже могут быть актуальными. Сюда же можно отнести контроль очередей на кассах с автоматическим уведомлением ответственного лица и оперативным привлечением дополнительного кассира, а также анализ наличия товара на полке с автоматическим уведомлением ответственного за выкладку.

Максим Максимов, "Аккорд-СБ"

Главная задача – полная съемка всех событий. Крайне важно иметь всю картину происходившего для установки степени ответственности каждого участника. Видеонаблюдение рассматривается как вспомогательная мера, помогающая в выполнении персоналом поставленных задач, защищающая как их самих, так и товарно-материальные ценности от третьих лиц. Будучи "всевидящим оком", видеонаблюдение в каждой точке призывает вести себя в рамках закона и установленных правил.

Какие модули видеоаналитики наиболее эффективны в ритейле для целей безопасности и маркетинга?

Евгений Золотарев, "Делетрон"

Можно выделить несколько популярных и несколько пока только набирающих популярность модулей видеоаналитики.

Среди популярных, которые решают исключительно потребности бизнеса, – контроль очереди и перемещения покупателей по торговому залу, включая аналитику этих процессов. К этой категории также можно отнести модули безопасности – контроль оставленных предметов и кассовых операций.

Набирающие популярность модули для бизнеса – это контроль выкладки товаров и свежести продуктов с аналитикой процессов, а для безопасности – распознавание лиц, трекинг перемещения по залу, поиск по заданным параметрам и аналитика по шоплифтингу.



Максим Максимов
Технический эксперт по видеонаблюдению ГК "Аккорд-СБ" ("Аккордтек")

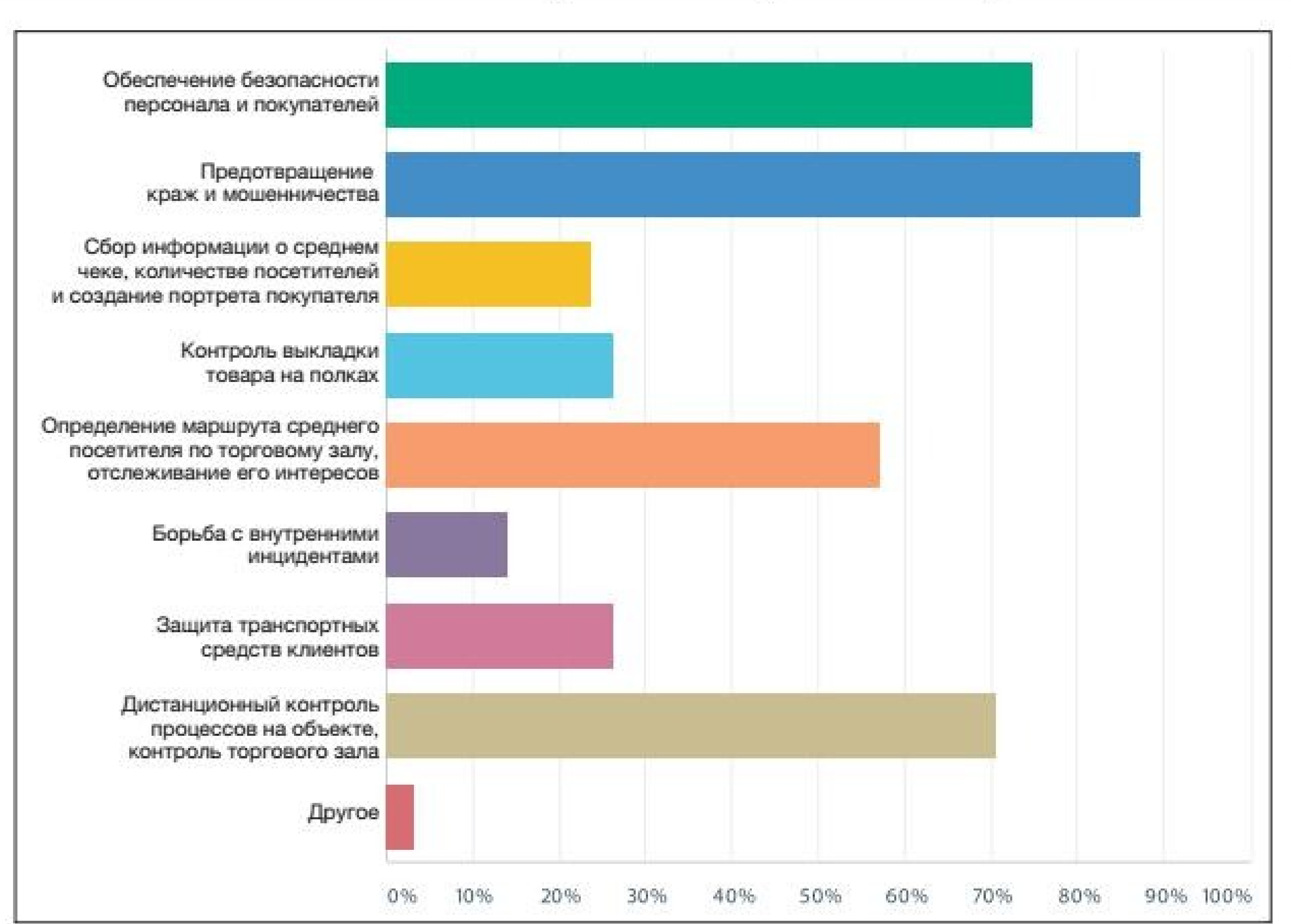
Артем Романов, КРОК

Для целей безопасности наиболее эффективен, как ни парадоксально, базовый детектор движения. Именно он позволяет определить проникновение постороннего в торговую точку в нерабочее время или его присутствие в служебном помещении. Автоматически выявить в режиме реального времени факт воровства в работающем магазине системы пока не могут, а вот зафиксировать ограбление ночью – запросто. Отсюда и эффективность.

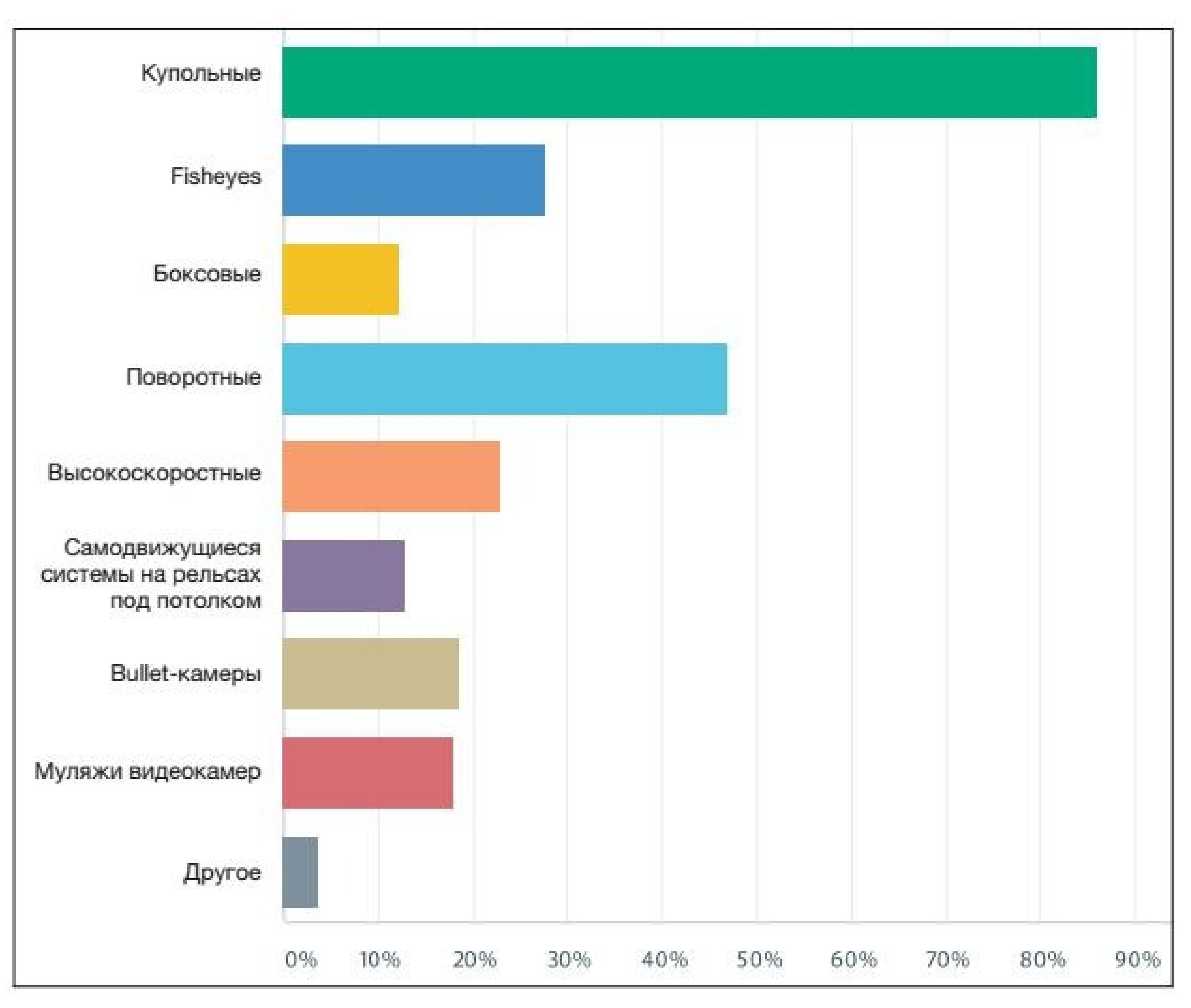
С маркетинговыми задачами ситуация сложнее, ведь эффективность зависит не столько от модуля видеоаналитики, сколько от корректности поставленной задачи и релевантной цели. Система соберет информацию для тепловой карты, но изменить расстановку стеллажей с товарами она не предложит. Или, например, она отследит эмоции на лицах посетителей, но не ответит на вопрос, почему они именно такие. Но зато система видеоаналитики может сама определить, что товар на полке заканчивается, и выдать предупреждение об этом. Поэтому подобный модуль я считаю эффективным, хоть он еще и не очень распространен.

Максим Максимов, "Аккорд-СБ"

В данный момент это детекторы движения на малопроходимых объектах, складах. Экономят время нахождения события также детекторы пересечения линии, вхождения и выхода из зоны. Умение делать подсчет людей в обозначенной области облегчает понимание загруженности отделов и персонала. Один из наиболее перспективных в ритейле – модуль наличия товара на полках. Распознавание и работа с базой лиц может быть использована для быстрого поиска конкретного человека, выдачи дополнительного сигнала персоналу и службе охраны магазина при его появлении в зоне действия камер.

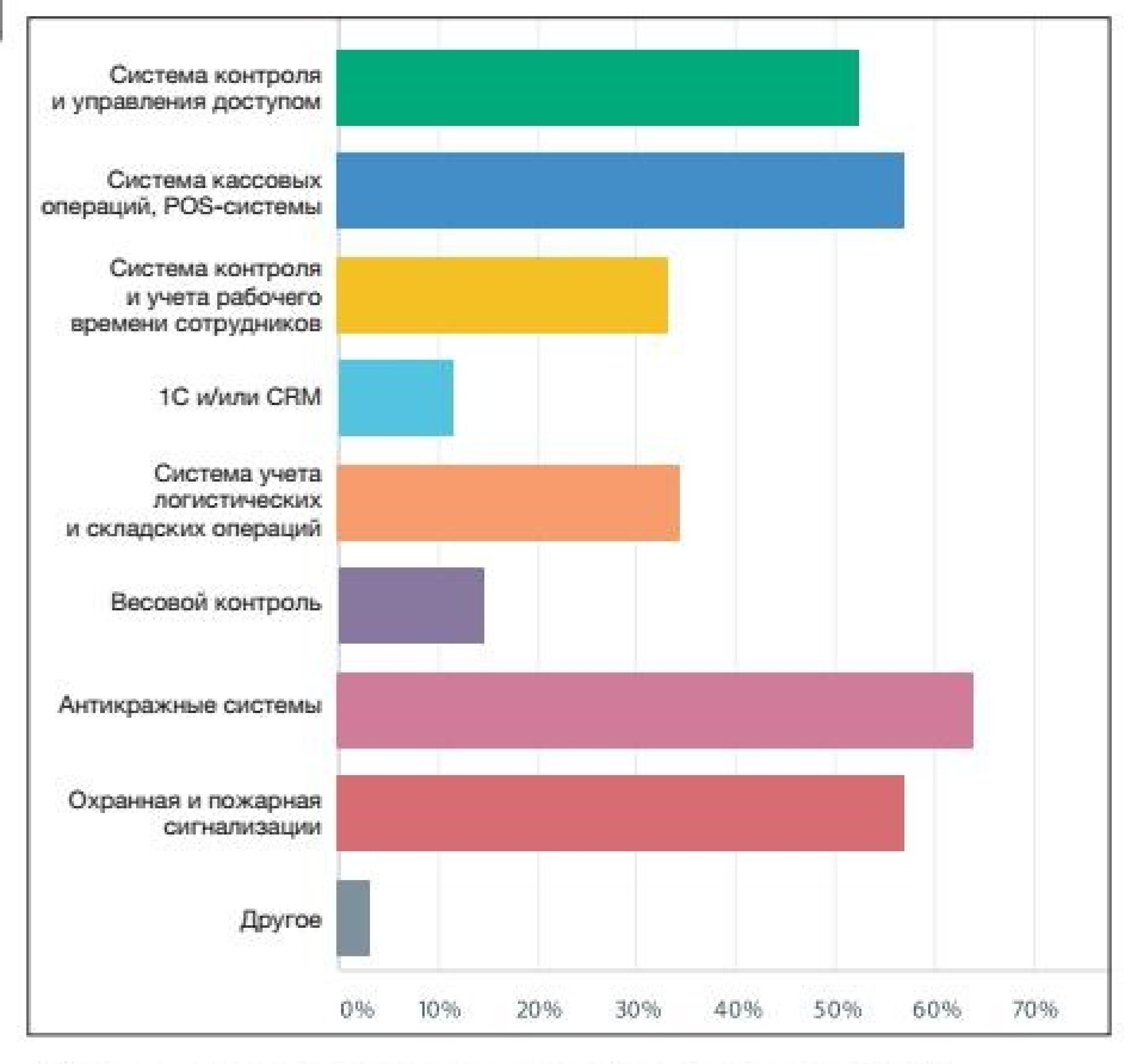


Задачи видеонаблюдения в ритейле*

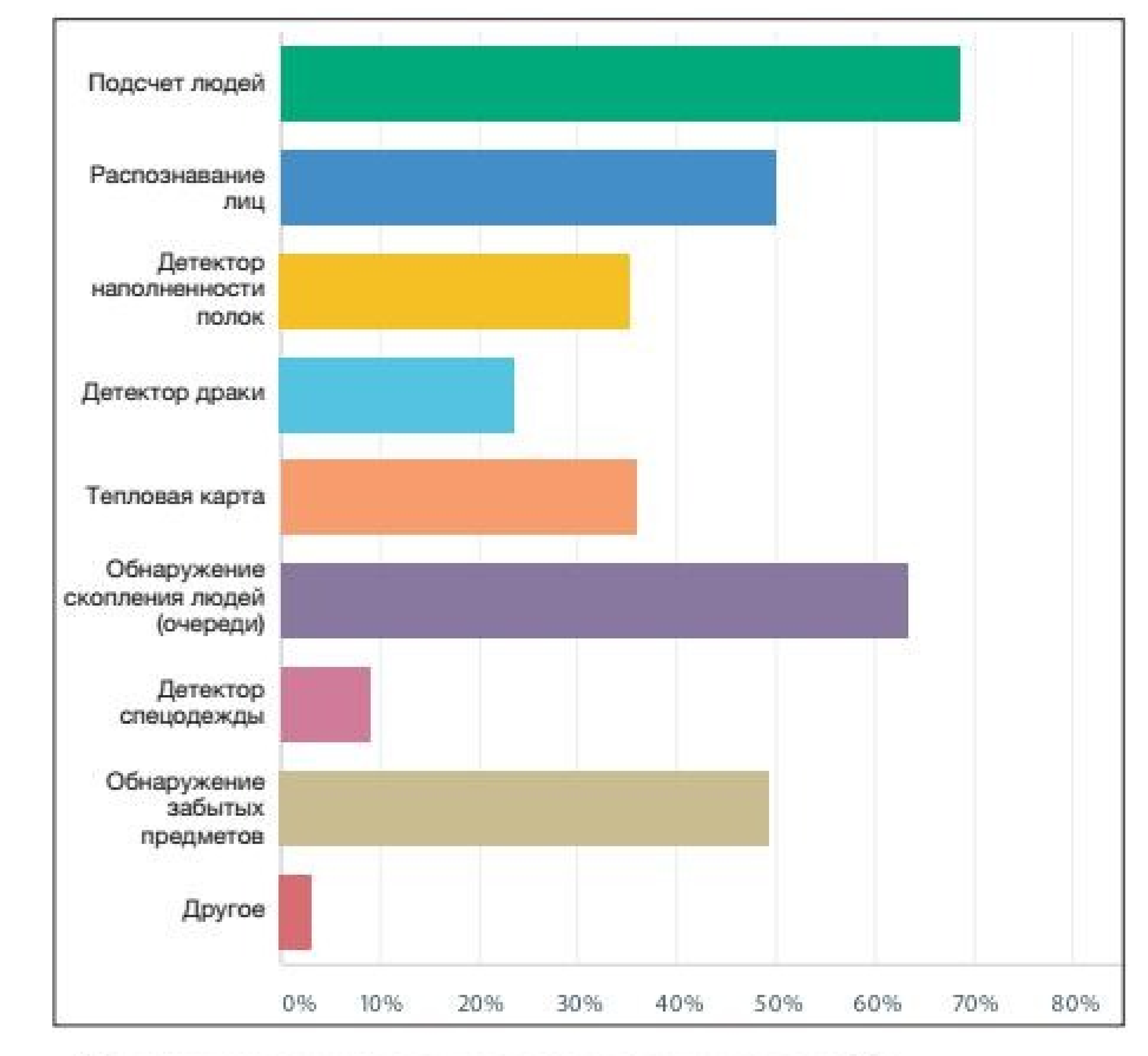


Оптимальные типы видеокамер для ритейла

** Графики построены на основе результатов опроса, проведенного редакцией журнала "Системы безопасности", и отражают мнение аудитории издания. Респонденты могли выбирать несколько вариантов ответов.*



С чем нужно интегрировать видеонаблюдение в ритейле?



Распространенные модули видеоаналитики в ритейле

Камеры в каком исполнении оптимально использовать в ритейле? Чем это обосновано?

Евгений Золотарев, "Делетрон"

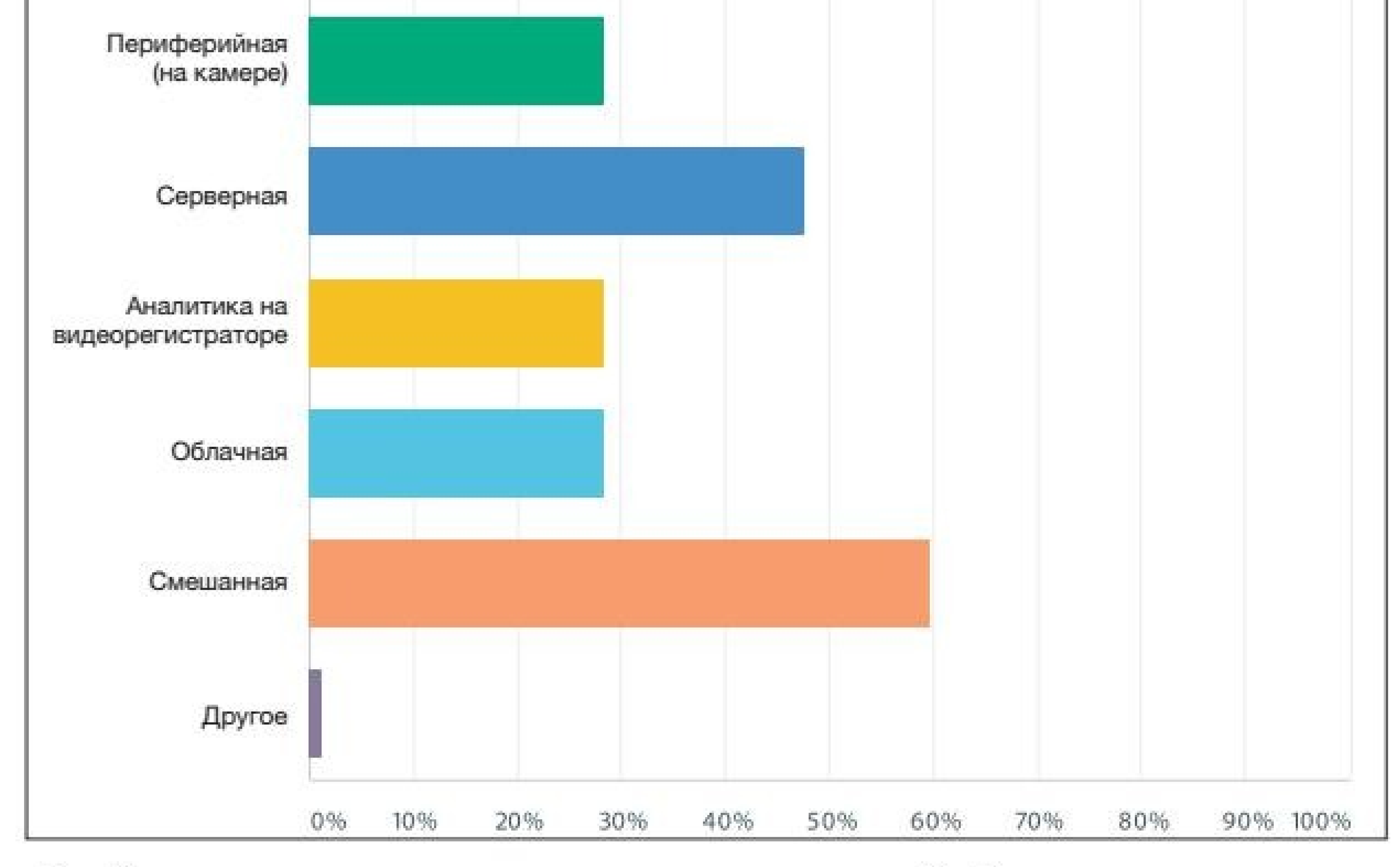
В связи с прогрессивными изменениями в производстве камер универсальными можно назвать купольные антивандальные моторизированные камеры с разрешением 4 Мпкс и функциями видеоаналитики на борту, системой захвата лиц, распознаванием лиц, идентификацией человека, а также встроенной аналитикой начального уровня (пересечение линий, вход/выход из/в зону и др.).

Артем Романов, КРОК

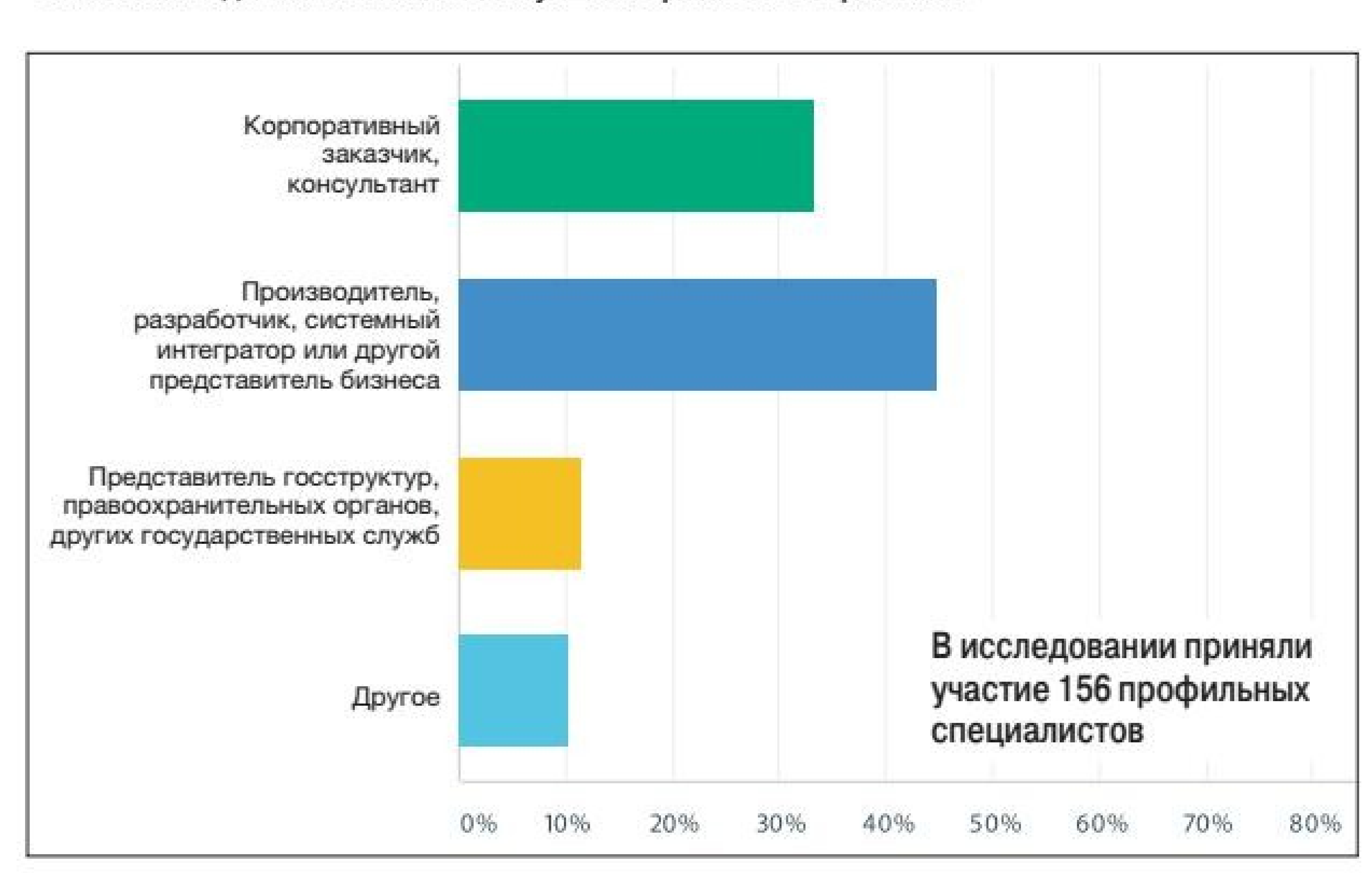
Исполнение камер определяется не типом объекта или отраслью, а задачей и местом установки каждой конкретной камеры. Наиболее универсальными считаются купольные камеры, но сказать, что для ритейла подходят только они, было бы неверно. Не везде можно установить их правильно, и не везде они смогут решить поставленную задачу. Где-то может потребоваться поворотная видеокамера или камера типа "буллит".

Максим Максимов, "Аккорд-СБ"

Оптимальный формфактор – компактные купола внутри помещений. Вне помещения – цилиндры. Внутри большое внимание уделяется внешнему виду, аккуратному и компактному исполнению, грамотному монтажу. Для уличных камер на первый план выходит техническая составляющая – высокая детализация изображения при различных условиях освещенности.



Какой тип видеоаналитики имеет лучшие перспективы в ритейле?



Роль респондентов на рынке систем безопасности

МНЕНИЕ ЭКСПЕРТА

Видеонаблюдение в ритейле: от контроля процессов до стратегических решений



Максим Захаров
Системный архитектор системы CVC компании "Кибер Айконтрол"

Основной задачей видеонаблюдения в ритейле, как и в большинстве индустрий, является предоставление фактуры для принятия управленческих решений касательно фронт- и бэк-офиса. При этом, на мой взгляд, эти решения могут и должны носить как тактический, оперативный характер при разборе конкретных противоправных действий или нарушений правил, так и стратегический при оценке выполнения персоналом процедур и регламентов.

Ритейлу нужны "работающие" модули видеоаналитики

В условиях, когда многие ИТ-компании декларируют все более расширяющийся спектр различных решений, важным аспектом становятся реальные возможности предлагаемых технологий, которые, к сожалению, нередко драматически отличаются от обещаний.

В разрезе маркетинга стоит посмотреть модули трафика/конверсии, особенно актуальными они будут на объектах, находящихся в ТРЦ. Видеоаналитика на основе нейросетевых роботов может стать отличным решением для контроля процессов на складах/логистических терминалах, а также при приемке товара на локализованном объекте. Результатом ее внедрения, помимо пресечения административных и экономических нарушений, должна стать оптимизация OPEX-расходов на персонал.

Экономическое обоснование прежде всего

Я бы удивился конкретному ответу от специалиста на данный вопрос – "Какое исполнение камер оптимально использовать в ритейле?". Все зависит от конкретных задач и проработанности экономического обоснования. Так, например, необоснованным может оказаться решение по замене аналоговых камер на IP: при значительном протяжении кабельных трасс и их исправном функционировании в данном случае нужно внимательно изучить возможность инсталляции AHD-/HDTVi-решений. При оснащении нового объекта необходимо учесть будущую роботизацию видеонаблюдения и не собрать дорогую, но заведомо устаревшую систему.

4 причины, почему распознавание лиц несильно сократит потери

Система распознавания лиц с базой данных магазинных воров не может существенно снизить потери в розничной торговле, и на это есть как минимум несколько причин:

1. Вход в магазин не похож на КПП с турникетом, а значит, выбор ракурса и требования к оборудованию станут технической и экономической проблемой.
2. На данный момент даже перспективные системы РЛ не способны распознать лица в масках в реальных, "боевых" условиях.
3. Существуют многочисленные сообщества шоплифтеров, которые довольно быстро опубликуют простые рекомендации, нивелирующие эффект таких систем.
4. Масса вопросов к стандартизации хешей лиц нарушителей, ведению такой базы и ее оперативному апдейту, причем это относится как к централизованным, так и децентрализованным системам.

Видеоаналитика для бизнес-процессов

В интеграции других систем с видеонаблюдением в текущем технологическом укладе смысла я не вижу, а вот с видеоаналитикой стоит интегрировать все основные системы автоматизации бизнес-процессов, начиная от кассовых систем и систем приемки на объекте и заканчивая WMS и клиринг-системами логистических терминалов.

см. стр. 120 "Ньюсмейкеры"

Может ли система распознавания лиц с базой данных магазинных воров существенно снизить потери в розничной торговле?

Евгений Золотарев, "Делетрон"

Да, может, и у нас уже есть такой опыт. Мы запустили систему распознавания лиц магазинных воров в российской сети магазинов, предварительно проведя анализ экономической эффективности такого решения еще в 2020 г. Естественно, для внедрения подобного решения розничный магазин должен вести статистику потерь от краж, так как есть вероятность, что потери от краж для различных форматов ритейла могут быть несопоставимы с потерями от неправильного хранения, логистики, краж со стороны сотрудников, даже от расстановки в зале. И возможно, в таком случае система распознавания лиц для снижения потерь не принесет значительного результата для бизнеса.

Сейчас мы тестируем разработку зарубежных коллег, которая выявляет подозрительную активность еще до совершения кражи, на основе более чем 100 аспектов поведения покупателей, включая походку, движения рук, мимику и даже выбор одежды, а также "замечает" ряд подозрительных действий, от беспокойного поведения до складывания предметов в сумки или карманы. Если она обнаруживает поведение, которое считает подозрительным, предупреждает персонал магазина через приложение на смартфоне. Затем сотрудники должны принять меры; обычно они обращаются к потенциальным ворам и спрашивают, нужна ли им помощь. Даже простое приветствие потенциального вора сотрудником магазина снижает риск кражи на десятки процентов.

Артем Романов, КРОК

Чтобы существенно снизить потери, одной только системы распознавания с базой данных недостаточно. Значительное снижение, очевидно, произойдет, если перестанут воровать. Логично, что для этого надо либо не пускать воров в магазины, либо добиться неотвратимости наказания. А значит, необходим еще ряд организационных и правовых мероприятий, причем не только от магазина. Приставить же к каждому потенциальному вору сопровождающего или установить систему видеонаблюдения с полным покрытием всего магазина со всех ракурсов экономически почти всегда нецелесообразно. Поэтому собственникам остается искать баланс между количеством потерь и стоимостью мер, направленных на их снижение. В целом я связываю потенциальное сокращение случаев воровства не с системами видеонаблюдения, а с более совершенным контролем за товаром или с новыми технологиями досмотра людей.

Максим Максимов, "Аккорд-СБ"

Может снизить, но только при одном условии: если на это лицо будет реакция сотрудников магазина, службы охраны, органов правопорядка. Без этого система не несет пользы.

Какие системы желательно интегрировать с видеонаблюдением в ритейле?

Евгений Золотарев, "Делетрон"

Все AI-системы предиктивного анализа, решающие бизнес-задачи и задачи безопасности. Начать надо с контроля кассовых операций, а заканчивать предиктивным анализом ситуаций, наличия и оценки качества товаров на витринах, а также поведения покупателей.

Артем Романов, КРОК

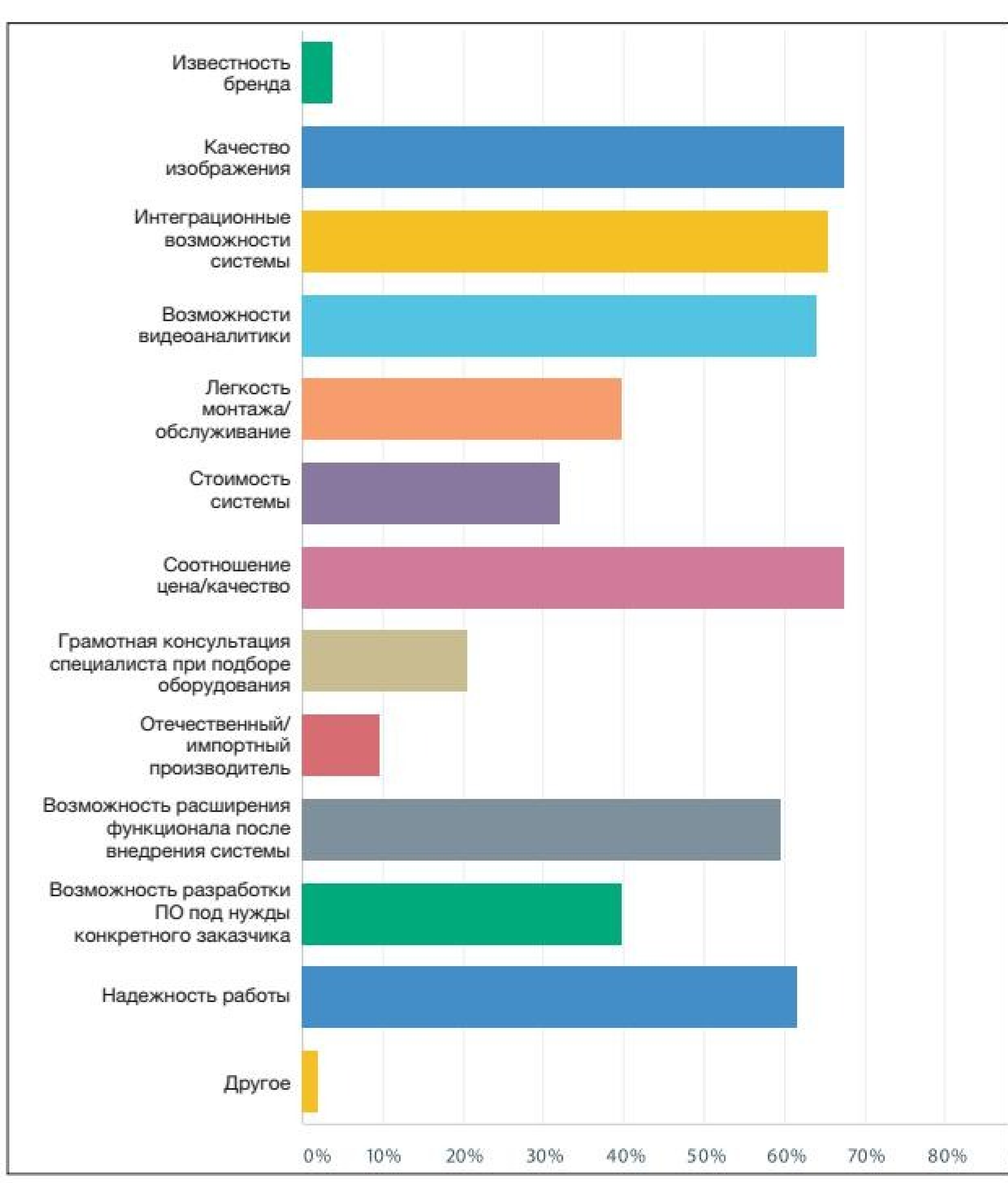
Интегрировать желательно те системы, события из которых помогут не допустить нарушения или злоупотребления. Интеграция с системой контроля кассовых операций позволит верифицировать фактический товар с пробиваемым артикулом. Система контроля и управления доступом даст информацию о том, чей пропуск или код доступа используется для входа в помещения.

Интеграция с инженерными системами здания поможет быстро среагировать, скажем, на сигнал "Пожар" от датчика пожарной сигнализации.

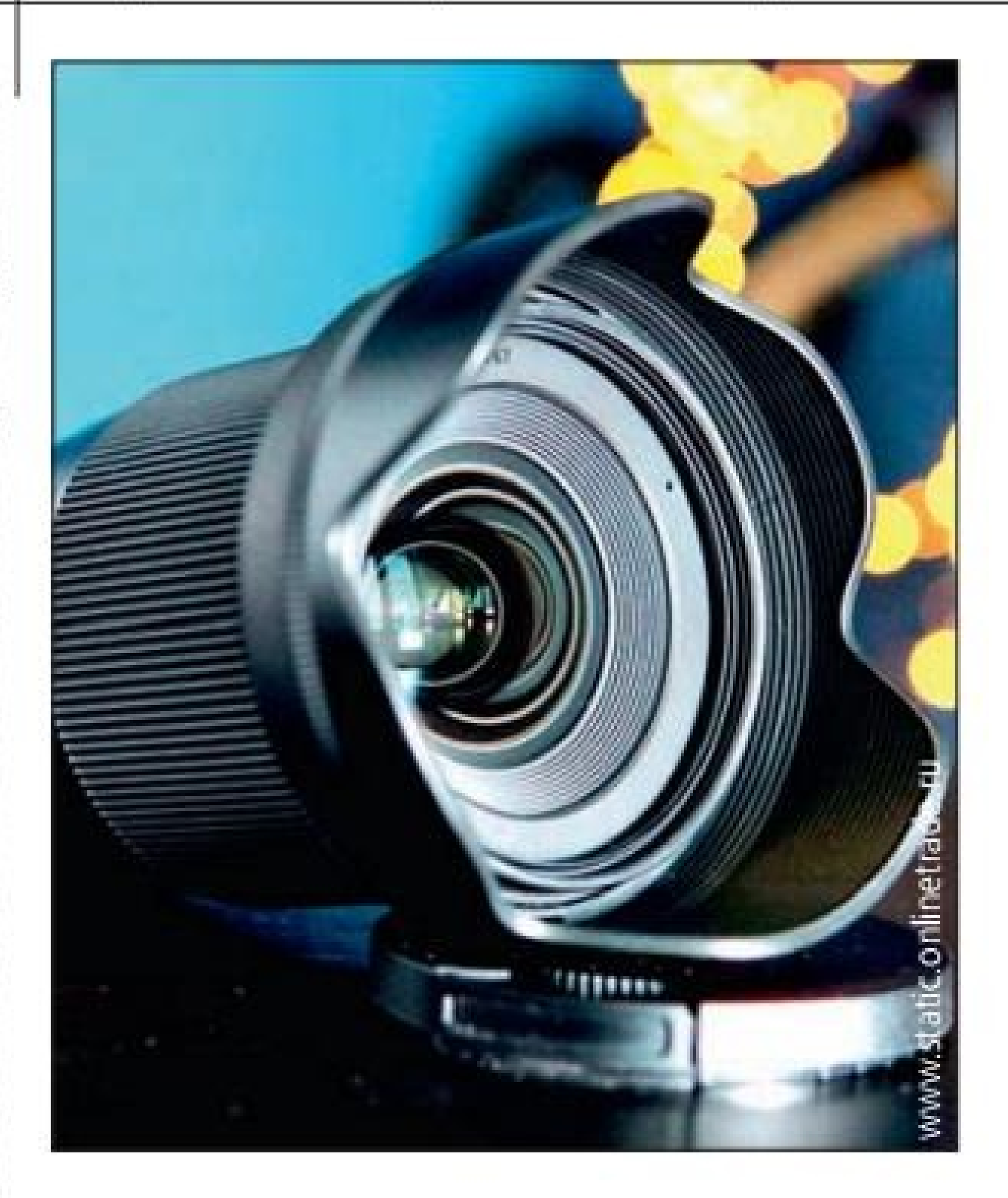
Как правило, это не соответствует текущей политике большинства ритейлеров по снижению издержек, но магазины самообслуживания, которые будут появляться в ближайшее время, без такой интеграции обойтись не смогут.

Максим Максимов, "Аккорд-СБ"

1. Контроль кассовых операций – сопоставление внешнего вида товара с наименованием в чеке (пробитым штрихкодом).
2. Дублирование сигналов систем СКУД, ОПС. Если запись ведется не на постоянной основе – задействовать тревожные входы записывающих устройств от данных систем для начала записи по наиболее значимым зонам/помещениям.
3. Возможность предоставить онлайн-доступ к видео охранным компаниям для принятия решения о выезде к месту событий. ■



Важные факторы при выборе системы видеонаблюдения для ритейла



Объективы для камер видеонаблюдения

Мнения экспертов

Реализация функциональных возможностей современных видеокамер и генерация видеопотока с четкой детализированной картинкой во многом зависят от объектива. Формат, технические характеристики, грамотная настройка – эти параметры объектива влияют на эффективность работы системы видеонаблюдения и решение конкретных задач безопасности. Эксперты из компаний "АРМО-Системы", "Фирма "Видеоскан" и "Болид" оценили текущую ситуацию на рынке в области объективов, объяснили востребованность одних устройств и почти полное исчезновение других, а также дали профессиональные рекомендации по выбору подходящих технологий



Роман Баранов
Бренд-менеджер компании "АРМО-Системы"



Николай Чура
Технический консультант компании "Фирма "Видеоскан"



Евгений Гуменюк
Начальник сектора технических средств видеонаблюдения ЗАО "НВП "Болид"

В каких случаях оправданно использование отдельных сменных объективов?

Роман Баранов, "АРМО-Системы"

Существует ряд задач, для наиболее эффективного решения которых целесообразно индивидуально выбрать камеру (матрицу), объектив и кожух. Использование сменных объективов оправдывает себя в тех случаях, когда технические характеристики интегрированного изделия недостаточны либо его цена выходит за рамки бюджета. Например, требуется высокая светосила объектива, большая кратность зума или оборудование будет использоваться в агрессивной либо взрывоопасной среде. Еще один пример – создание своего уникального решения, не имеющего прямых аналогов. Здесь уместно провести аналогию с мультитулом и набором специализированных инструментов.



Отдельные сменные объективы часто используются в камерах машинного зрения

Николай Чура, Фирма "Видеоскан"

Самый простейший случай – когда в силу внешних причин вы располагаете видеокамерой под сменный объектив либо подобная камера по своим характеристикам более предпочтительна. Другой вариант – если требуется оптика с повышенной светосилой, большей кратностью изменения фокусного расстояния как в ручном, так и в дистанционно управляемом режиме (зум). Но в любом случае отдельный объектив, как и отдельная камера, как бы предполагают более высокое качество продукта.

Евгений Гуменюк, НВП "Болид"

Применение отдельных сменных объективов предпочтительно при использовании корпусных камер или камер машинного зрения, которые конструктивно не имеют встроенного объектива. Прежде всего это нужно для задач, требующих применения камер, обладающих специфическими характеристиками, в специальных защитных кожухах, либо когда требуется объектив с свойствами, недоступными встроенным аналогам. Например, трансфокаторы с фокусными расстояниями более 100 мм.

Почему на рынке преобладают видеокамеры со встроенным объективом?

Роман Баранов, "АРМО-Системы"

Преобладание интегрированных изделий связано с тем, что они позволяют решить основные задачи, подходят для большинства ситуаций. Интегратор тратит меньше времени на сборку системы, а если, к примеру, объектив моторизованный и камера имеет функцию автофокуса, то экономит время на пусконаладке. Однако на рынке присутствуют и моторизованные объективы C- и CS-mount, что в некотором роде дает второе дыхание сборным системам, поскольку проектировщики и интеграторы не ограничены готовыми решениями, имеют больше выбора и пространства для творчества.

Николай Чура, Фирма "Видеоскан"

Стремление к камерам со встроенным объективом обусловлено несколькими причинами.

Снимается проблема оптимального подбора отдельных узлов системы, требующего более широкого предложения этих узлов и высокой квалификации как проектировщика, так и исполнителя проекта.

Эта задача еще больше усложняется при необходимости использования защитного бокса и устройств дополнительной подсветки, особенно в случае невидимой инфракрасной (ИК) подсветки.

Евгений Гуменюк, НВП "Болид"

Основными причинами преобладания видеокамер со встроенным объективом являются низкая стоимость при равном качестве изображения и отсутствие необходимости подбора подходящего объектива. Подавляющее число систем видеонаблюдения не требуют применения видеокамер с особыми возможностями, к тому же сейчас на рынке достаточно камер для специальных задач или условий эксплуатации.

Видеокамеры развиваются, становятся универсальнее, получают более длиннофокусные и скоростные объективы, климатические модули, антикоррозионные и взрывозащищенные корпуса. При сравнительно невысокой стоимости такие видеокамеры позволяют проектировщику не задумываться о подборе подходящего объектива и оболочки к камере. Эта тенденция способствует дальнейшему вытеснению корпусных видеокамер и объективов к ним с рынка охранного видеонаблюдения.

Возможно ли в ближайшем будущем массовое возвращение объективов большого формата?

Роман Баранов, "АРМО-Системы"

На данный момент наиболее массовый формат матрицы в системах видеонаблюдения – 1/2,8–1/2,7" с разрешением 2–5 Мпкс. Следующий по популярности – ½–1/1,7" с 5–12 Мпкс. Как правило, чем больше матрица, тем больше должен быть объектив и тем они дороже. Технологии не стоят на месте, однако на сегодняшний день формат крупнее 1/1,8" (2/3", 4/3" и т.д.) используется прежде всего в системах технического зрения. Объективы и матрицы больших форматов вполне могут стать более востребованными в CCTV в будущем, если это, к примеру, даст существенные преимущества для видеоаналитики (позволит успешнее детектировать интересующие события в автоматическом режиме, уменьшит зависимость системы от оператора) или даст возможность заменить несколько камер меньшего формата.

Николай Чура, Фирма "Видеоскан"

Главным препятствием применения объективов большого формата, кроме их массогабаритных характеристик, является крайне высокая стоимость. Рост цены для оптики подчиняется почти такому же

"ужасному" закону, как и в сенсорах. Кратность роста апертуры приводит к росту цены почти в четвертой степени кратности. Но стремление к применению больших форматов изображения (4K и 8K) подталкивает к вынужденному росту форматов как датчиков изображения (CCD- или CMOS-матриц), так и применяемой оптики. Здесь можно возразить, что в достаточно серьезных гаджетах (айфонах и смартфонах) уже давно применяются миниатюрные матрицы на 8, 12 и более мегапикселей с миниатюрной же оптикой. Однако задача видеонаблюдения – обеспечить максимально возможное качество изображения при минимальной освещенности. Причем всевозможные цифровые "примочки", как накопление по времени или площади, шумоподавление или цифровая коррекция четкости при субъективном улучшении картинки, в реальности уменьшают пространственное и временное разрешение изображения.

Объективы и матрицы больших форматов вполне могут стать более востребованными в CCTV в будущем, если это, к примеру, даст существенные преимущества для видеоаналитики (позволит успешнее детектировать интересующие события в автоматическом режиме, уменьшит зависимость системы от оператора) или даст возможность заменить несколько камер меньшего формата

Евгений Гуменюк, НВП "Болид"

Вполне возможно, в первую очередь вслед за активным развитием и внедрением камер машинного зрения. Матричные и линейные камеры высокого разрешения оснащаются сенсорами более крупного формата для обеспечения оптимальной детализации. Камеры машинного зрения становятся все более востребованными в таких сферах, как интеллектуальные системы дорожного движения (ИТС), промышленный контроль, спорт, аэрофотосъемка и т.д. Это достаточно перспективное направление, которое способствует развитию и продвижению рынка высокотехнологичных объективов большого формата.

Применение сверхширокоугольных объективов и панаморфной оптики растет или сокращается?

Роман Баранов, "АРМО-Системы"

Сверхширокоугольные или Fisheye-объективы применяются в потолочных камерах, вызывных панелях домофонов. Чаще всего они создают эквидистантную (равнопромежуточную) проекцию изображения. Недостатком таких решений можно назвать значительное искажение геометрии и сжатие объектов по краям кадра до трудноразличимых размеров, эффект дверного глазка. Панаморфные объективы используют стереографическую (равноугольную) проекцию, за счет чего изображение по центру выглядит не настолько выпукло, а по краям не настолько сжато, как у классических Fisheye. Благодаря этому общая детализация картинки существенно выше и она гораздо лучше подходит для развертки в панораму и виртуальных туров. Это также важно для задач маркетинга (подсчета посетителей, построения тепловых карт и т.д.). В борьбе за покупателя производители упомянутых устройств переходят на панаморфную оптику, тем самым повышая качество продукта.

Николай Чура, Фирма "Видеоскан"

Создается впечатление, что после рекламной лихорадки применение сверхширокоугольных объективов и панаморфной оптики несколько поутихло. Камеры, позволяющие с помощью подобных объективов осуществлять практически круговое наблюдение одним сенсором, поначалу сильно воодушевили инсталляторов. Серьезным препятствием для их применения стало весьма низкое качество изображения, несмотря на серьезную цифровую коррекцию. Особенно это характерно для бюджетных моделей. Целесообразность получения погонного разрешения изображения, эквивалентного формату D1 от камеры с сенсором в 5 Мпкс, вызывает серьезные сомнения. В этом случае стоимость нескольких достаточно бюджетных камер HD или даже FullHD "перекачивается" в сложную и дорогую оптику, а также программное обеспечение.

Евгений Гуменюк, НВП "Болид"

С увеличением количества камер, применяемых для обзора больших пространств (вокзалов, аэропортов и стадионов), растет и потребность в сверхширокоугольных объективах. Но из-за их специфики детализация видеоизображения далека от идеала, да и работа с таким изображением требует специальных возможностей от средств просмотра. При должном развитии программного обеспечения, позволяющего лучше воспринимать картинку оператором, востребованность этих объективов будет увеличиваться. С другой стороны, сейчас на рынке активно развиваются мультисенсорные системы, которые лишены указанных недостатков и обеспечивают панорамное видеоизображение высокой детализации без искажений. Минусом таких систем является высокая цена. Если в будущем они подешевеют, то вполне способны вытеснить с рынка видеокамеры со сверхширокоугольными объективами.

Каковы особенности объективов для тепловизоров?

Роман Баранов, "АРМО-Системы"

Основным отличием тепловизионных объективов является рабочий диапазон спектра – 8–14 мкм вместо 0,4–0,9 мкм у цветных камер. Второе отличие – гораздо более широкий диапазон рабочих температур, например -40...+80 °C против стандартных -10...+50 °C. Третье – атермализация, или компенсация расфокусировки изображения, которая нарастает с отклонением температуры объектива от нормальной (+20...+25 °C). Для видимого спектра атермализацию можно встретить в некоторых трансфокаторах большой кратности, например x62. И наконец, тепловизионные объективы зачастую имеют более высокую светосилу (F0.95, F1.0), чем объективы видимого диапазона. Таким образом компенсируется недостаточная чувствительность тепловизионных сенсоров.

Николай Чура, Фирма "Видеоскан"

Объективы для тепловизоров принципиально мало чем отличаются от объективов видеокамер. Принципиальное отличие – это используемый материал, который должен быть прозрачен для ИК-излучения в диапазоне от 3 до 13 мкм (3000 до 13 000 нм). Обычно это германий (Ge) или реже селенид цинка (ZnSe). Ввиду очень дорогого материала стоимость объективов, особенно сложных и многоэлементных, крайне высока. В остальном они имеют те же самые составные части, диафрагму или механизм изменения фокусного расстояния ручного или моторизованного типа. Для объективов повышенной светосилы, а соответственно и большой апертуры зачастую применяются зеркальные сферические или даже асферические элементы.

Главным отличием объективов для тепловизоров является основной материал линз – это германий

Евгений Гуменюк, НВП "Болид"

Главным отличием объективов для тепловизоров является основной материал линз, из которого они производятся, – это германий. В отличие от стекла он пропускает излучение в диапазоне волн 1,8–23 мкм и имеет наивысший показатель преломления. Это позволяет применять такие объективы в тепловизионных системах, работающих в спектральном интервале 8–14 мкм. Важный параметр для неохлаждаемых тепловизоров – светосила, поэтому в таких камерах практически не применяются вариофокальные объективы.

Ожидает ли нас переход объективов на систему управления диафрагмирования P-Iris?

Роман Баранов, "АРМО-Системы"

Там, где это дает существенные преимущества, – в системах распознавания автомобильных номеров, лиц, где есть требования к стабильно высокому качеству изображения, переход с DC-Iris на P-Iris фактически уже произошел. Система DC-Iris по-прежнему несколько дешевле P-Iris и остается востребована в низкобюджетном сегменте. Справедливости ради стоит упомянуть и камеры с объективами M12 (S-mount), в которых диафрагма фиксирована и не управляется. Они также занимают свою нишу.



Николай Чура, Фирма "Видеоскан"

Технология P-Iris предназначена для предотвращения падения четкости изображения при глубоком диафрагмировании объектива. В стандартных условиях это происходит при глубоком диафрагмировании системы с автодиафрагмой в случае очень сильной освещенности. В аналоговых системах управления объектива камерой это было неизбежно. Две аналоговые системы стабилизации яркости изображения (видеосигнала) – автодиафрагма и электронный затвор не могли устойчиво работать одновременно. При цифровом управлении камеры появилась возможность по мере закрытия диафрагмы одновременно сокращать длительность электронного затвора.

В системах распознавания автомобильных номеров, лиц, где есть требования к стабильно высокому качеству изображения, переход с DC-Iris на P-Iris фактически уже произошел

Евгений Гуменюк, НВП "Болид"

Технология P-Iris способна обеспечить лучшую четкость, контрастность и разрешающую способность. Но так как она сложнее в реализации, многие производители предлагают такие камеры только в дорогих линейках оборудования, к тому же выбор совместимых объективов очень мал. Учитывая, что общий интерес к корпусным камерам и отдельным объективам неуклонно снижается и что за почти 10 лет существования данной технологии переход на нее так и не случился, ситуация останется на прежнем уровне.

Почему практически прекратилось широкое применение объективов Pinhole для скрытого наблюдения?



Схожие с Pinhole по конструкции объективы широко применяются в родственных видеокамерам устройствах – в вызывных панелях видеодомофонов

Роман Баранов, "АРМО-Системы"

Дело в том, что скрытое наблюдение в целом попало под законодательные ограничения и стало прерогативой спецслужб. Тем не менее схожие по конструкции объективы широко применяются в родственных видеокамерам устройствах – в вызывных панелях видеодомофонов.

Николай Чура, Фирма "Видеоскан"

Объективы Pinhole, то есть объективы с вынесенным зрачком малой апертуры, либо квази-Pinhole с сильно уменьшенной апертурой очень широко предлагались в 1990-е и начале 2000-х гг. Это обусловливалось высоким уровнем преступности и одновременно слабым контролем государства. Камеры и даже домофонные панели вырывались "с мясом" из стен и дверей буквально за несколько минут. Именно тогда в России родились видеоглазки, маскирующиеся под типовые оптические. Это исключало типовой "бытовой терроризм" стрельбой в открывшийся глазок. Использование таких объективов в камерах домофонов можно рассматривать как некий атавизм. Сейчас эти объективы отнесены к разделу спецтехники, применяются исключительно для скрытого получения информации и практически запрещены для частного использования.

Евгений Гуменюк, НВП "Болид"

В нашей стране широкому применению Pinhole-объективов препятствует законодательство. По закону об оперативно-розыскной деятельности такие камеры могут применяться только МВД, ФСБ и другими силовыми ведомствами. Их использование частными лицами запрещено ст. 137 и 138 УК РФ. Стоит заметить, что в последние 10–12 лет усилился контроль за покупкой и продажей подобных устройств. Поэтому компании, которые раньше занимались продажей таких камер, перестали их ввозить. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Александр Малинин
Глава российского представительства Seagate

Как развиваются технологии видеонаблюдения и меняется их восприятие

Решения для анализа данных видеонаблюдения применяются все шире

Первая функционирующая система видеонаблюдения появилась в Германии в 1942 г., однако на протяжении десятилетий эта технология имела весьма ограниченную сферу применения, используясь в основном для военных целей. В последнее десятилетие видеонаблюдение бурно развивалось и прочно вошло в самые различные сферы нашей жизни. Пандемия COVID-19 еще больше расширила области ее применения и функциональность, перед разработчиками и пользователями встали новые задачи

В условиях массового перехода на дистанционную работу, вызванного пандемией COVID-19, к системам видеонаблюдения стали предъявлять новые требования. Если раньше их в основном использовали, чтобы следить за дорожным движением и контролировать функционирование заводского оборудования, то теперь видеонаблюдение становится важным элементом в работе офисов с резко уменьшившейся численностью персонала, а также средством для обеспечения соблюдения социальной дистанции в магазинах и моллах.

Сфера применения технологий видеонаблюдения существенно расширилась, в том числе благодаря их применению совместно с многочисленными датчиками и устройствами Интернета вещей, работающими в круглосуточном режиме. Средства видеонаблюдения внедряются повсеместно: их используют службы безопасности университетов, школьные администрации, розничные торговые сети и даже специалисты по изучению диких животных.

Камеры видеонаблюдения генерируют огромное количество данных, их объем теперь измеряется терабайтами. Всю полученную информацию требуется сохранить и обеспечить к ней доступ для дальнейшего анализа, целями которого являются повышение рентабельности предприятий и скорости принятия решений, привлечение новых клиентов и оптимизация затрат. Например, стандартным требованием становится возможность поиска по сохраненным видеоданным. Как следствие, решения для видеонаблюдения становятся более гибкими и эффективными благодаря масштабируемости систем хранения данных и активному развитию программного обеспечения для управления видео и аналитикой на основе искусственного интеллекта. А особенности развертывания камер, использования систем хранения данных и ПО варьируются в зависимости от среды, для которой нужно обеспечить мониторинг.

Сферы наиболее активного применения систем видеонаблюдения

Университеты

Во многих странах кампусы и аудитории университетов сегодня пустуют: студенты и преподаватели в условиях пандемии учатся и работают в удаленном режиме. Для России это уже не так релевантно, но и у нас помещения не бывают заняты 24/7. Лабораторное оборудование становится все дороже, в аудиториях увеличивается количество техники, поэтому на фоне сложностей в экономике и растущей безработицы для них охрана актуальна как никогда.

Поскольку сохранять огромные объемы данных требуется ежедневно, университетские системы видеонаблюдения нуждаются в многотерабайтных хранилищах. Для них необходимы возможности масштабирования и применения современного ПО.



Видеонаблюдение остается основным компонентом безопасности образовательных учреждений

Розничная торговля

На протяжении всего 2020 г. ритейлеры были вынуждены постоянно менять свои бизнес-процессы. В условиях пандемии большинству из них приходится рассчитывать на то, что основную прибыль будут приносить онлайн-продажи. Вместе с тем видеотехнологии по-прежнему полезны для мониторинга маршрутов покупателей в торговых залах, уменьшения потерь и контроля товарного ассортимента.

Заботясь о здоровье покупателей, многие продавцы предлагают бесконтактную доставку.



Камеры используются и для контроля за соблюдением покупателями антиковидных ограничений

В помещения магазинов покупателей пускают лишь небольшими группами, за соблюдением ими социальной дистанции приходится постоянно следить. Видеонаблюдение, как и раньше, используется для охраны товаров на полках, но теперь также и для обеспечения безопасных условий труда работников и охраны здоровья гостей.

Промышленность

Круглосуточное видеонаблюдение необходимо и на производственных предприятиях. Нередко промышленные площадки находятся вдали от головного офиса, и, соответственно, их оборудование можно определить как периферийные системы. Камеры играют важную роль в мониторинге удаленных площадок, они служат не только для обеспечения безопасности, но и для обнаружения поломок.

За последние годы количество датчиков, установленных на заводских линиях, существенно выросло, соразмерно увеличился объем генерируемых данных. Анализ показаний датчиков помогает руководству оперативно отслеживать ситуацию в заводских цехах. Надежное хранение и защита этих данных являются необходимым условием для использования современного ПО, реализующего функции искусственного интеллекта и машинного обучения. Таким образом, сегодня системы видеонаблюдения не только выполняют для предприятий роль органов зрения и слуха, но и помогают обеспечивать бесперебойную эксплуатацию удаленных объектов.

Защита диких животных

Многие виды диких животных сегодня находятся под угрозой исчезновения, и дистанционное видеонаблюдение за ареалами их обитания помогает оберегать их. Сегодня, в частности, действуют системы наблюдения за бизонами в США, носорогами в Африке, белыми медведями на Аляске, тропическими птицами в Южной Америке и пандами в Китае.

Постоянный мониторинг жизнедеятельности и отслеживание миграции животных помогают ученым принимать решения о мерах по защите видов, находящихся на грани вымирания. Так системы видеонаблюдения способствуют охране и изучению дикой природы и помогают защищать животных от браконьеров.

Умные города

Последние в нашем списке, но первые по значимости, города остаются основным драйвером развития видеонаблюдения и технологии искусственного интеллекта по обработке входящего видеопотока. Благодаря интеграции с системой мониторинга трафика и умными светофорами видеокамеры помогают регулировать движение, обеспечивать контроль за соблюдением ПДД и прибывать спасательным службам на место, тратя на 20–30% меньше времени. Уличное видеонаблюдение делает города безопасными, а наказание для преступников – неотвратимым. Когда человек знает, что его правонарушения точно будут запечатлены, то желание совершать антиобщественные поступки значительно уменьшается. По статистике, наличие таких систем видеонаблюдения снижает преступность на 30–40%.

Постепенно камеры становятся качественнее, а видеопоток занимает больше места. Учитывая, что правоохранительным органам иногда нужно обратиться к записи с конкретной камеры, сделанной пару месяцев назад, встает вопрос о хранении всего этого постоянно увеличивающегося массива информации.



В последнее время все чаще применяется видеонаблюдение с искусственным интеллектом

Сфера применения технологий видеонаблюдения существенно расширилась, в том числе благодаря их применению совместно с многочисленными датчиками и устройствами Интернета вещей, работающими в круглосуточном режиме. Средства видеонаблюдения внедряются повсеместно: их используют службы безопасности университетов, школьные администрации, розничные торговые сети и даже специалисты по изучению диких животных

Ценность данных видеонаблюдения для бизнеса

Данные создаются, используются и анализируются на всех этапах жизненного цикла систем видеонаблюдения, от проектирования и развертывания и до повседневной эксплуатации. В отчете Seagate Rethink Data, опубликованном в 2020 г., убедительно показана эффективность использования больших объемов данных для повышения производительности бизнес-процессов в самых разных отраслях экономики.

Большую роль в этом играют системы видеонаблюдения, применение которых варьируется от обеспечения безопасности до реализации сложных решений на основе искусственного интеллекта. По данным отчета, в частности, в Европе датчики автомобилей на автопилоте генерируют колоссальные массивы данных, от 5 до 20 Тбайт в день на одно транспортное средство. Весь объем этой информации должен быть доступен бортовому интеллектуальному ПО в режиме реального времени, чтобы избегать аварий. Эта информация также нужна в периферийных системах автомобильных компаний для максимально быстрого анализа рабочих характеристик беспилотных транспортных средств. Именно поэтому высокоэффективным интеллектуальным инфраструктурам данных для систем видеонаблюдения сегодня придается такое большое значение.

Обеспечение доступа к данным – необходимая мера, которую нужно предпринять уже сейчас ради ускорения инноваций вне зависимости от того, в каких условиях развертываются системы видеонаблюдения. Если говорить о будущем, то в числе приоритетных целей поставщиков оборудования – повышение точности, эффективности и надежности продукции нового поколения, которая создается для эпохи экономики данных.

Взгляд в будущее

Бесперебойный доступ к данным, ускорение инноваций, повышение точности, эффективности и надежности систем видеонаблюдения – приоритетные задачи организаций в рамках обеспечения безопасности офисных помещений и жилых домов в 2021 г. и в будущем.

Тема видеонаблюдения требует особого отношения, ведь камеры следят за офисами, зданиями и другими объектами в круглосуточном режиме, передавая информацию, которая позволяет обнаруживать различные угрозы, предотвращать потери и поломки локального и удаленного оборудования. Видеонаблюдение способствует оптимизации бизнеса, в том числе помогает улучшать предоставляемые сервисы и выявлять недоработки.

Пришло время провести ревизию применяемых систем хранения данных на соответствие современным требованиям к емкости и плотности записи и экономии электроэнергии. Кризис, вызванный пандемией COVID-19, ускоряет процессы миграции в облако и внедрения гибридных приложений, соединяющих центры обработки данных с удаленными системами. Видеонаблюдение сегодня немыслимо без возможности хранить огромные объемы данных, а в связи с массовым переходом на облачные вычисления хранилища должны быть максимально быстрыми и энергоэффективными. Если ваши системы хранения данных не отвечают этим требованиям, значит, пришло время обратить внимание на более современные решения, позволяющие внедрить эффективные и экономичные бизнес-процессы, охватывающие дата-центры, облака и периферию. ■

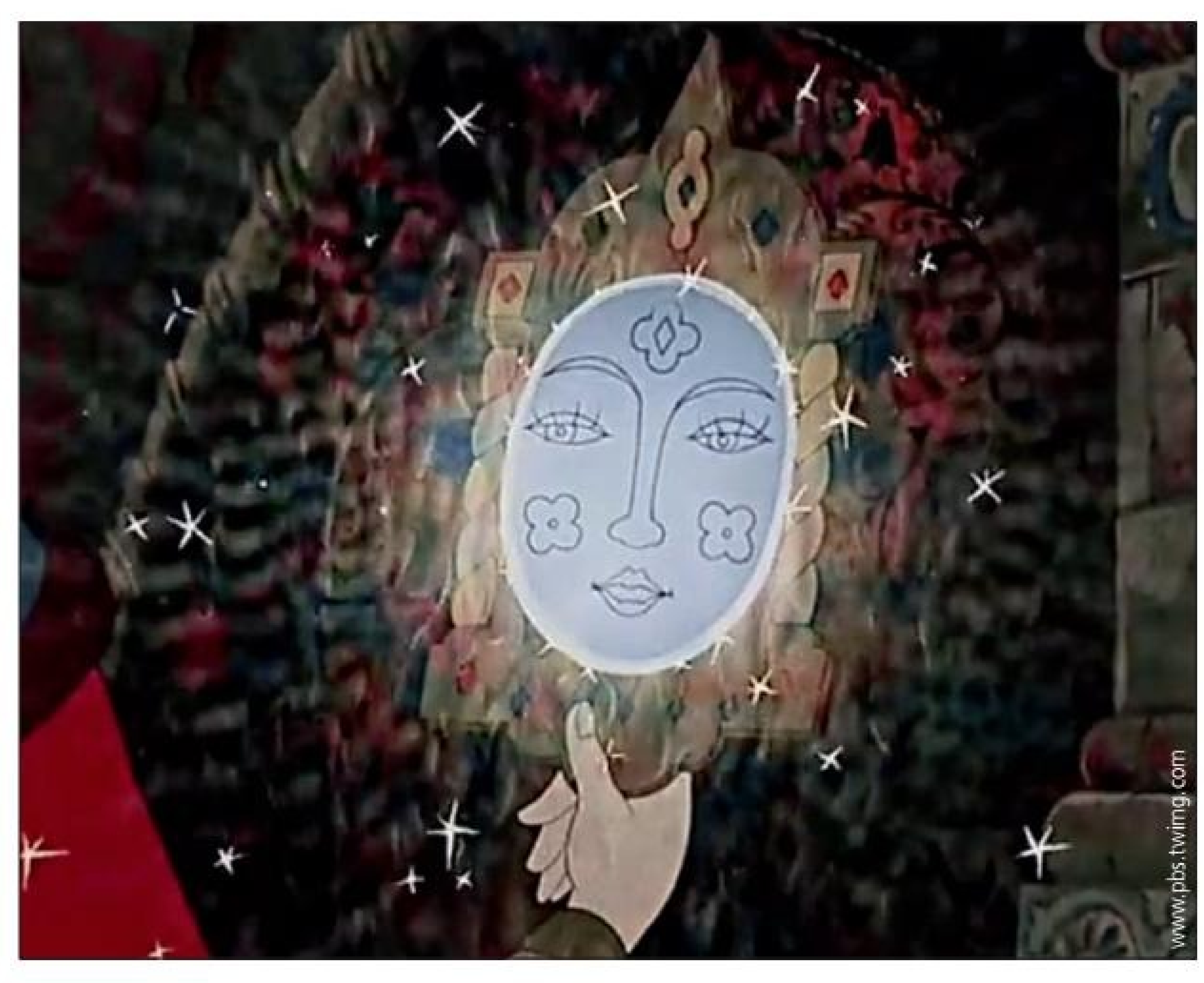
Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Валентин Пашинцев
Ведущий специалист Центра сервисного обслуживания ГУ МВД по Московской области

От соглядатаев до IP-технологий
История видеонаблюдения

Современные видеокамеры поражают своими возможностями. Они могут давать обзор в 360 град. , находить, зуммировать и вести объект, работать в полной темноте и распознавать лица людей. С чего началась история видеонаблюдения, что изменилось за последние 20 лет?



Волшебное зеркало – сказочный прообраз современных средств видеонаблюдения

На протяжении всего времени своего существования человеку было важно знать, что происходит за пределами его жилища. Неандерталец, прежде чем выйти наружу, потихоньку выглядывал из пещеры, проверяя, нет ли поблизости опасных зверей. Правителю (вождю, князю, фараону, царю) более развитого общества необходимо было знать, что происходит на подвластных ему землях. Подобная информация собиралась в двух целях:

- открытый сбор сведений велся для контроля происходящего в стране, слежения за ходом работ при строительстве пирамид, дворцов, плотин и т.д.;
- тайное получение информации было направленно на нейтрализацию внешних и внутренних угроз государству.

Прообразы средств видеонаблюдения

До создания электронных средств видеонаблюдения их роль выполняли люди. В городах это были соглядатаи, агенты, работающие на службы правопорядка, – полицейские, стражники, центурионы. При сооружении крупных объектов – надсмотрщики и мастера. Они докладывали руководителю, а тот правителю, что хочет подвластный ему народ и что необходимо властелину, чтобы удержаться на троне. Правители, которые были глухи к народным нуждам, часто заканчивали свою жизнь на эшафоте. Большую опасность для монархов представляло и их окружение. Правящая элита часто вступала в заговор с целью посадить на трон своего кандидата. Свергнутого монарха редко оставляли в живых. Таким образом, если он хотел жить, то должен был знать и контролировать намерения своих близких подданных.

Чтобы раскрывать заговоры, пользовались услугами тайных агентов, а также средствами слежения тех времен: тайными глазками в стенах, особыми слуховыми коридорами для прослушивания разговоров в комнатах гостей.

В различных источниках встречается также упоминание о приборе, через который король мог наблюдать, что происходит в тронном зале. Скорее всего, речь идет о системе зеркал, установленных под углом в 45 град., с помощью которых и передавалось изображение. Позже такой способ использовался в перископах подводных лодок.

Мечты видеть на расстоянии отражались в сказках. Хрустальный шар, волшебное зеркало, тарелочка с наливным яблочком – это не что иное, как сказочные прообразы современных средств видеонаблюдения.

Первые приборы для передачи изображений на расстояние

В XX веке сказки о ковре-самолете, хрустальном шаре, самодвижущейся повозке и других волшебных предметах стали превращаться в реальность.

Первое в мире устройство, способное передавать картинку на расстоянии, создал в 1931 г. в США русский инженер Зворыкин. Своему изобретению он дал название "иконоскоп" (от греческих слов eikn – изображение и skopo – смотрю).

В иконоскопе изображение с объектива поступает на мозаику, состоящую из множества конденсаторов, один вывод которых подключен к глобуле серебра, а другой к "земляному" выводу. В результате на конденсаторах накапливается заряд, пропорциональный падающему на мозаику свету.

Далее электронный луч, образованный системами развертки и фокусировки, пробегает по экрану, считывая видеосигнал.

Позже иконоскопы были заменены более чувствительными и совершенным передающими телевизионными трубками. Это суперортиконы, видиконы и некоторые другие.

28 ноября 1933 г. инженером Шмаковым был изобретен супер-иконоскоп. Он на порядок превосходил чувствительность иконоскопа Зворыкина.

Отечественная камера КТП-67 1975 г. выпуска была оборудована видиконом и объективом "Юпитер-М", имела моторизированный фокус и управляемый поворотный механизм. Размер камеры был обусловлен использованием видикона. Для его работы требовались блоки строчной и кадровой развертки, блок высокого напряжения, блок синхронизации, и все это на дискретных элементах.



Иконоскоп Зворыкина – первое устройство, способное передавать изображение на расстояние

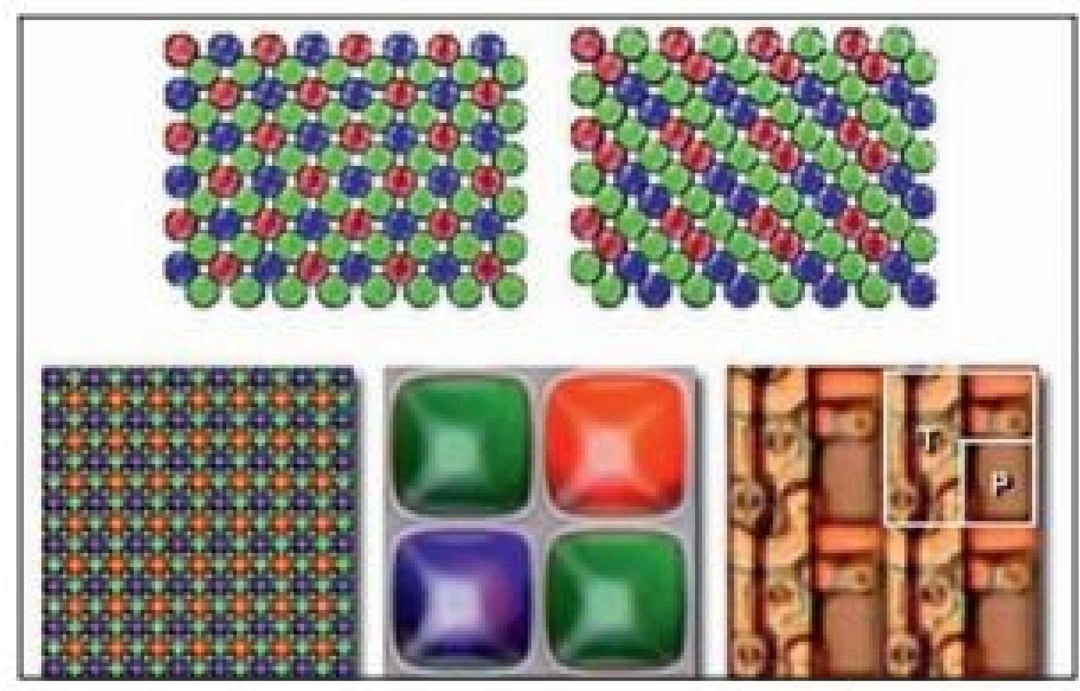


Видеокамера КТП-67 1975 г. выпуска

Технические характеристики:
- **чувствительность 0,1 лк;**
- **разрешение от 380 до 420 телевизионных линий;**
- **угол обзора от 3,4 до 90 град;**
- **угол обзора при использовании поворотного устройства до 360 град;**
- **питание 24 В;**
- **потребляемый ток 250 мА;**
- **длина 390 мм, ширина 220 мм, высота 140 мм;**
- **Вес 4 кг**

Матрицы камер видеонаблюдения

Четкость изображения видеокамеры зависит от используемого в ней светочувствительного сенсора (матрицы). Размер камер сильно уменьшился после появления матриц CCD (ПЗС, прибор с зарядовой связью). Они были изобретены в 1969 г. Уиллардом Бойлом и Джорджем Смитом в Лабораториях Белла (AT&T Bell Labs). Способность элемента памяти матрицы принять заряд благодаря фотоэлектрическому эффекту дала возможность сделать использование ПЗС в видеонаблюдении основным. В 1970 г. у исследователей из Лабораторий получилось снимать картинку с помощью простых линейных устройств.



Матрицы разделяют цветное изображения на составляющие

Под воздействием света в любом пикселе матрицы возникают электроны. В течение заданного промежутка времени все пиксели постепенно заполняются электронами, пропорционально количеству попавшего в него света. По окончании этого времени электрические заряды, накопленные определенным пикселем, по очереди подаются на "выход" прибора и измеряются.

Таким образом, для каждого последующего момента времени мы можем получить значение накопленного заряда и определить, какому пикселю на матрице (номер строки и номер столбца) он соответствует.

Вначале использовались монохромные матрицы. Позже их заменили цветные. Так как ночью невозможно получить качественное цветное изображение, применялся специальный фильтр, переводивший камеру в черно-белый режим в условиях плохой освещенности.

Используя специальные фильтры матрицы, разделяют цветное изображения на составляющие.

Камеры на основе ПЗС матриц использовались в течении многих лет, но возросла скорость процессоров видеокамеры, и связанное с этим появление мегапиксельных камер привело к тому, что скорость последовательного сканирования стала недостаточной. Поэтому производители были вынуждены перейти на КМОП-матрицы (КМОП – комплементарная структура "металл – оксид – полупроводник", англ. CMOS).

CMOS-технология предусматривает размещение электронных компонентов непосредственно в любом пикселе светочувствительной матрицы. Главное преимущество технологии – малое энергопотребление в статическом состоянии. Это дает возможность использовать такие матрицы в составе энергонезависимых устройств, например в датчиках движения и системах наблюдения, находящихся большую часть времени в режиме сна или ожидания события.

Важным преимуществом матрицы КМОП является единство технологии с остальными, цифровыми элементами аппаратуры. Это приводит к возможности объединения на одном кристалле аналоговой, цифровой и обрабатывающей части, что послужило основой для миниатюризации камер для самого разного оборудования и снижения их стоимости ввиду отказа от дополнительных процессорных микросхем. Возможность считывания нужных групп пикселей резко убыстрила обработку изображения.

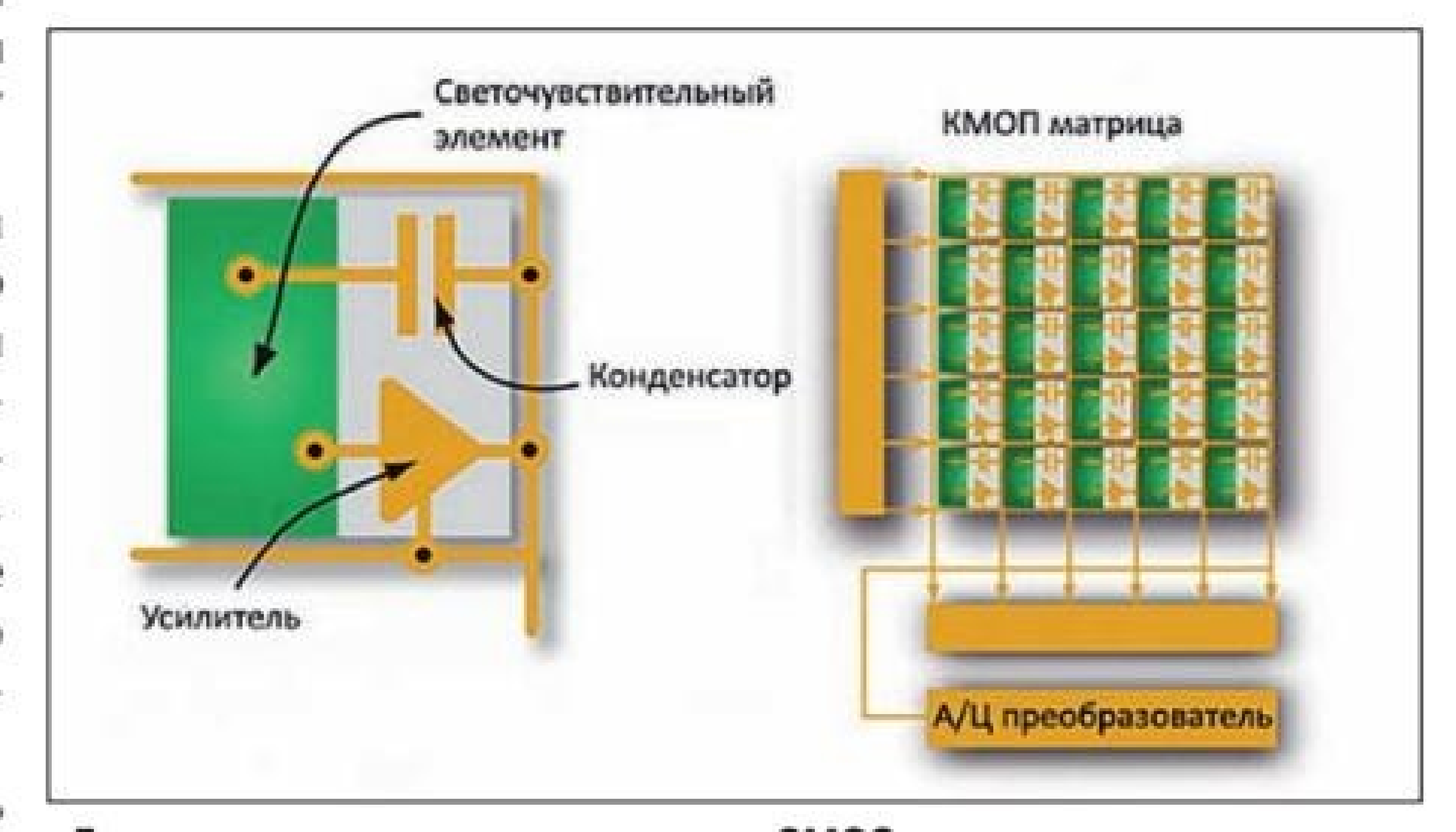
Дополнительные усилительные схемы могут быть размещены в любом месте по цепи прохождения сигнала. Это позволяет улучшить работу камеры в условиях недостаточного освещения. Возможность изменения коэффициента усиления для каждого цвета улучшает балансировку белого.

Производство КМОП-матриц намного дешевле в сравнении с ПЗС-матрицами, особенно при больших размерах матриц.

К 2008 г. КМОП практически заменили ПЗС.

Видеонаблюдение началось с дорог

С момента изобретения передающей трубки Зворыкина до ее реального применения прошло четверть века. Только в 1956 г. в Гамбурге



Главное преимущество технологии CMOS – малое энергопотребление в статическом состоянии

были применены видеокамеры для управления движением на перекрестках. Полицейский видел дорожную ситуацию на мониторе и по мере надобности переключал светофор.

В 1959 г. в Ганновере и Мюнхене видеонаблюдение стало применяться для контроля, ставшего более интенсивным уличного движения. В 1965 г. система видеофиксации на улицах Мюнхена была расширена до 14 камер, каждая из них имела возможность дистанционного управления поворотом и трансфокатором.

В 1968 г. в США, в городе Олен, была впервые применена система видеонаблюдения для охраны территории складов. Правда, для создания 8-камерной системы потребовалось два года и 1,5 млн долларов. Но, несмотря на высокую стоимость, идея стала популярной.

Посты видеонаблюдения оснащались десятками мониторов: каждой камере был нужен свой. Операторам было трудно контролировать такое количество экранов, их внимание рассеивалось. Поэтому появились первые устройства мультиплексирования – квадраторы. Они объединяли четыре исходных видеосигнала в один общий. На мониторе выводилась картинка, состоящая из четырех изображений, каждое из которых представляла собой уменьшенное отображение с одной из видеокамер. Это дало возможность резко уменьшить количество экранов в центре видеонаблюдения.

С появлением мониторов с большими экранами появилась возможность применять в видеосистемах мультиплексоры, работающие с 8, 9, 16 камерами. По своим возможностям они подразделялись на три вида:

- симплексные мультиплексоры позволяли только просматривать изображения;
- дуплексные мультиплексоры обеспечивали просмотр изображения и запись его на видеомагнитофон;
- триплексные мультиплексоры – просмотр изображения, запись на видеомагнитофон и просмотр сохраненного контента.

Устройства видеозаписи

С появлением первых видеосистем возникла потребность в сохранении полученной информации. Оператор должен был, не отрываясь, следить за изображением на мониторах, чтобы не пропустить ничего важного.

В 1951 г. появились первые VTR-устройства (Video Tape Recorder), записывающие изображение на магнитную ленту. Размером они были со шкаф и стоили немало. Первый видеомагнитофон, созданный в 1956 г., был способен полноценно записывать звук и изображение на магнитную ленту при помощи магнитных видеоголовок, но стоил при этом 50 тыс. долларов. Однако это не помешало стремительному росту популярности устройства: уже через полгода видеомагнитофон стал применяться во всех ведущих телевизионных студиях США. Но до охранных видеомагнитофонов было еще далеко.



Появление квадраторов дало возможность уменьшить количество экранов в центре видеонаблюдения

Таблица. Характеристики IP-камер разных годов выпуска

Параметр	2009	2011	2015	2019
Чувствительный элемент	1/3" ПЗС	1/4" КМОП	1/3" КМОП	1/2.9" КМОП
Разрешение (пикс.)	720x576, 352x288	20x576	1280x1024	1920×1080
Чувствительность (лк)	0,15	Ч/б 0,1	Цв. 0.1	Цв. 0,05
Стандарт сжатия	MPEG4_ASP	H.264, M-JPEG	H.264, MPEG-4	H.264, H.265
Макс. фреймрейт: (кадр/с)	25	30	30	60

Охранные видеорегистраторы предназначены для записи событий, контролируемых системой видеонаблюдения. Основное отличие охранных видеомагнитофонов от бытовых – возможность записи на стандартную (обычно трехчасовую) видеокассету в течение длительного времени (до 960 часов), а в случае тревоги переход на более качественную видеозапись.

Охранный видеомагнитофон обеспечивает работу в различных режимах, с его помощью можно искать запись, сделанную в определенное время или день, а также записи событий с тревогой. По принципу работы в режиме длительной записи охранные видеомагнитофоны различались на Time Lapse (прерывистая запись) и Real Time (видеомагнитофоны реального времени), отличающиеся записью меньшего количества кадров в секунду, чем в поступающем видеосигнале.

Сейчас такие видеомагнитофоны уже не применяются, они вытеснены устройствами цифровой записи. Мультиплексор с записью на жесткий диск – это то, что мы называем видеорегистратором. С развитием технологий емкость и скорость считывания винчестеров все время увеличивались. Сейчас их емкость достигает 2 Тбайт, при скорости 100 Мбит/с. Это дает возможность записывать большие объемы информации.

Из личного опыта

Когда в 2000 г. я начал заниматься видеонаблюдением, еще доживали свой век советские камеры, подобные описанным выше КТП-67. Качество картинки было очень низким. Если днем еще можно было что-нибудь рассмотреть, то ночью мы видели только светлые пятна от фонарей. В других подразделениях нашей организации были черно-белые камеры оборудованные ПЗС-матрицами импортного производства. Использовались также квадраторы и дуплексные мультиплексоры. Особо важные участки записывались на видеомагнитофон. Единой системы видеонаблюдения у нас не было.

Централизованное оборудование Московской области системами видеонаблюдения началось с 2005 г. Система безопасности представляла собой модульное программное обеспечение, связанное по схеме трехуровневой клиент-серверной модели. В комплект поставки входили две платы на четыре канала видео и звука каждая. По тем временам система обладала хорошими характеристиками:

- аппаратное сжатие;
- аппаратный детектор движения (до 100 зон детекции на канал);
- формат видео изображения и записей – mpeg-4 (стандарт H.264);
- поддерживаемые разрешения: 352/288 (CIF), 704/288 (HD1), 704/576 (D1);
- до 25 кадр/с по каналу независимо от разрешения;
- переменный/постоянный (с возможностью выбора) битрейт;
- синхронный звук по всем каналам.

К 2007 г. вся область была оборудована подобными системами. Однообразие оборудования позволило облегчить обслуживание и ремонт.

IP-системы

В 2007 г. появилась первая ласточка IP-систем. Она представляла собой переходное устройство между аналогом и IP. Основу четырехкамерной системы составляла большая камера, которая имела три входа для аналоговых камер и выход на UTP-линию. Внутри устройства сигнал от четырех камер оцифровывался и подавался на разъем для передачи на компьютер. К камере можно было подключить аналоговый монитор. Скорости передачи по витой паре не хватало, поэтому сигнал на изображении то и дело зависал. Но все-таки пара десятков этих устройств были установлены.

В 2009 г. у нас появилась полноценная система IP-видеонаблюдения. В комплект входили системный блок, свич, блок питания и четыре камеры. В комплект ПО входила утилита, с помощью которой обнаруживались IP-адреса камер. После их надо было прописывать в программе, с указанием параметров настройки.

Поскольку видеокамеры имели сравнительно небольшой битрейт, проблем с нагрузкой сети не возникало. Камеры подключали к свичу, находящемуся рядом с системном блоком.

В 2011 г. на вооружение поступила система, которая могла работать уже с 32 камерами, причем как с IP, так и с аналогом (при использовании дополнительных плат видео захвата). К ней можно было подключать до 10 клиентских рабочих мест.

В 2015 г. один сервер уже мог работать с 80 камерами, причем можно было использовать несколько серверов в одной системе. Система отличалась удобным интерфейсом и автоматической настройкой. Подключались также модули видеоаналитики.

В сравнительной таблице видно, как менялись характеристики устройств в последние 10 лет. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Максим Сорока
Генеральный директор
компании "Витэк-Автоматика"

Камера машинного зрения в промышленном исполнении

Этап тестирования готовой продукции

Камеры машинного зрения, зачастую работающие не в "тепличных" условиях эксплуатации, должны быть к этому готовы. В статье "Камера машинного зрения в промышленном исполнении. Воплощение замысла", опубликованной в № 1/2021 журнала, мы рассказали об особенностях конструирования промышленных камер машинного зрения. Сейчас пойдет речь об их производстве



Рис. 1. Пример цикла испытаний в климатической камере

Для того чтобы у вас в руках оказалась настоящая промышленная камера, необходимо должным образом воплотить идеи ее разработчиков в производстве серийного продукта.

Тщательному контролю качества подлежит каждая камера, именно он обеспечивает уверенность в функциональных возможностях, производительности каждого экземпляра и выявляет изделия с дефектами или функциональными отклонениями до того, как они попадут к заказчикам.

В первой статье мы упоминали об ускоренных методиках испытаний и тестов HALT (Highly Accelerated Life Tests) и HASS (Highly Accelerated Stress Screening). На примерах компании LUCID Vision Labs (Канада) мы продемонстрировали, как стресс-тестирование на основе HALT помогает сократить сроки разработки новых изделий. Теперь давайте рассмотрим аналогичный подход к контролю качества готовой продукции.

Стресс-тесты при контроле качества производства – далеко не общая практика. Стресс-тестирование согласно HALT и HASS, с одной стороны, ускоряет процесс, но с другой – требует значительных затрат на подготовку, выбор типов и обоснование объемов "стресса", постоянную работу по совершенствованию процедур. То есть в плане затрат происходит смещение акцентов от приобретения бо́льшего объема оборудования и более длительных традиционных тестов в сторону коротких, если угодно, "рискованных", но научно обоснованных, интеллектоемких подходов. Этим готовы заниматься далеко не все производители.

Надежность

Сразу стоит отметить, что любое тестирование сокращает ресурс готового продукта. Стресс-тестирование сокращает его, пожалуй, в большей степени. В чем же тогда преимущество метода HASS? Самое главное – HASS позволяет быстрее и с меньшими затратами (стоимость оборудования) выявить максимальное количество дефектов. Давайте попробуем разобраться, как этого эффекта достичь, причем без ущерба для функциональных возможностей устройства.

Современные методы разработки электроники, в том числе и с помощью стресс-тестов HALT, в комбинации с доступными материалами позволяют создавать продукты с запасом прочности, во много раз превышающим необходимый. Однако набор стресс-тестов нужно ограничить теми, которые, конечно же, "съедают" определенную долю ресурса, но при этом оставшаяся часть не только достаточна, но и обладает запасом для работы оборудования с расчетной максимальной нагрузкой в течение запроектированного срока жизни. Большинство дефектов материалов и компонентов носят кумулятивный характер, а именно проявляются по мере накопления "усталости". То есть чем сильнее нагрузка в начале эксплуатации, тем больше вероятность проявления таких дефектов за определенный отрезок времени. В этом, собственно, и заключено основное преимущество метода HASS: он позволяет выявить максимальное количество дефектов в кратчайшие сроки с минимальными затратами, и обязательно без значимого ущерба для ресурса изделия. Обеспечение достаточности остаточного ресурса – один из важнейших критериев, согласно HAAS. Давайте обратимся к практикам уже известной нам компании LUCID Vision Labs.

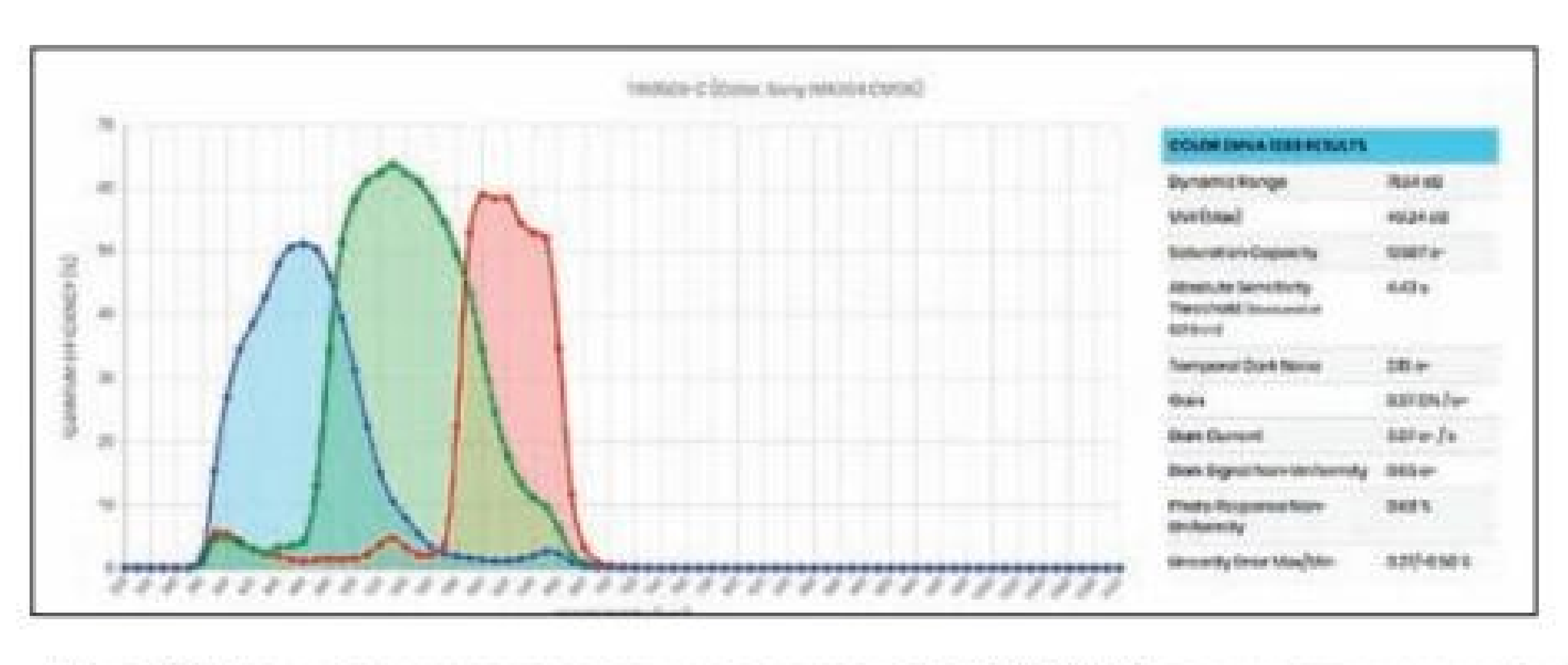
Самые очевидные нагрузки – это резкое изменение температуры в климатической камере, или термоудар. Каждое изделие подвергается циклическому воздействию в климатической камере с перепадом температур от высокой до низкой. Речь не идет, конечно же, о доведении конструкции до разрушения, как это происходит на этапе разработки, но пороги все равно устанавливаются с небольшим превышением рабочих температур, чтобы гарантированно достичь их уровня. Во время температурных циклов периодически выполняется функциональное тестирование: включение/выключение питания, захват и передача изображений, проверка корректности контрольной суммы (CRC) chunk'ов и соотношения "сигнал/шум" (SNR). Контролируется соответствие номинальным значениям величины потери данных (Bit Errors) и потребления электроэнергии.

Циклические испытания в климатической камере продолжаются несколько часов и помогают выявить изделия с дефектами прежде, чем они попадут в руки заказчика. Помимо этого, подтверждается их работоспособность в заданном широком диапазоне температур, от -20 °C для камер LUCID Triton и Atlas.

В случае если камеры обеспечивают уровень защиты IP67, как LUCID Triton и некоторые модели Atlas, проводятся испытания на предмет защиты от проникновения влаги и пыли. Соответствие классу защиты IP67 (стандарт IEC 60529) предполагает, что камера должна быть пыленепроницаема и выдерживать 30-минутное погружение на глубину до 1 м. Для сокращения времени контроля качества изделий выполняются тесты методом погружения под давлением.

Качество изображения

Важнейшим контролируемым параметром камеры машинного зрения является качество изображения, которое, помимо прочего, опре-



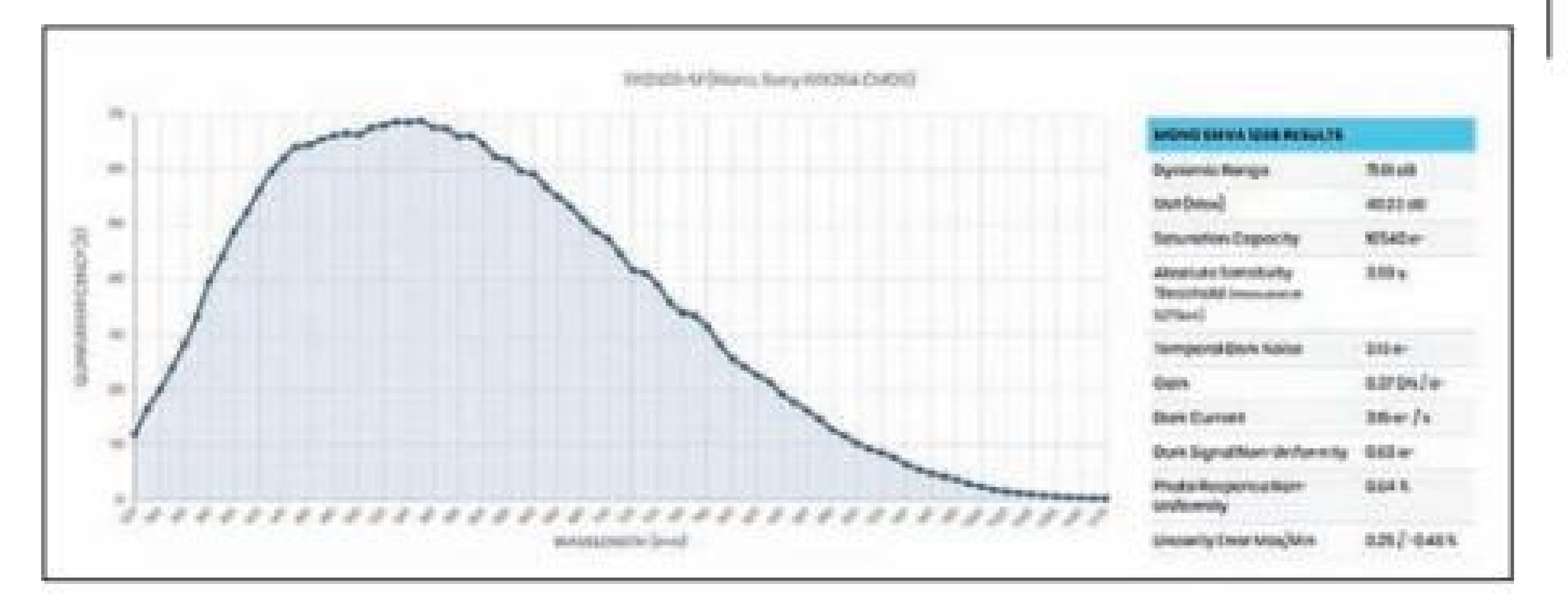


Рис. 2. Пример характеристик согласно EMVA1288 для цветных и монохромных камер

деляется точностью установки сенсора относительно оптической оси и фокальной плоскости объектива. По сравнению с обычным механическим позиционированием матрицы, с применением прокладок и пассивных техник, процедура центровки Active Sensor Alignment обеспечивает более точное положение сенсора относительно отверстия объектива. Это критически важно, особенно в случае крупноформатных камер, для ясного и резкого изображения по всей плоскости сенсора от центра на периферию и стабильного качества изображения от камеры к камере. Наклон плоскости сенсора относительно оптической оси приводит к разнице значений фокусного расстояния в зависимости от удаленности от центра. Смещение может привести к затенению углов. Поворот усложняет процедуру установки камеры на объекте.

Объективную картину качества изображения дает тест с использованием источника равномерного излучения (Flat Field) в соответствии со стандартом EMVA1288 (EMVA, European Machine Vision Association – Европейская ассоциация машинного зрения). Результаты тестов должны укладываться в заданный для данной модели диапазон. Измеряются уровень темнового шума и его неоднородность, емкость насыщения, неоднородность фоточувствительности, нелинейность. Измерения подтверждают стабильность рабочих характеристик от изделия к изделию. Образец, не прошедший тесты, изымается и отправляется на дополнительные испытания. Поскольку большинство производителей камер тестируют свою продукцию в соответствии со стандартом EMVA1288, пользователи на основании результатов испытаний могут сравнивать качество изображения камер с разными сенсорами от многих поставщиков. Наличие характеристик качества изображения в соответствии с EMVA1288 на сайте производителя камер – очевидный индикатор его отношения к качеству своего продукта.

Заключение

Не все камеры машинного зрения предназначены для использования в суровых условиях промышленного производства, поэтому при выборе оборудования для этих целей необходимо прежде всего определить критерии, которым оно должно соответствовать. Производитель, помимо деклараций о готовности к работе на производстве в режиме 24/7, должен представить соответствующие стандарты и результаты испытаний. Настоящий материал представляет собой лишь краткий обзор подходов, призванных обеспечить надежность и функциональность камер машинного зрения для промышленных и аналогичных им условий применения. Инновационные продукты в промышленном исполнении – база наиболее надежных и долговечных систем машинного зрения, создаваемых вами для своих заказчиков. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА ЭКСПЕРТА



Тенденции безопасности

Вынужденный двухгодичный перерыв между выставками Securika Moscow явно отразился на посещаемости последнего форума: во второй и третий дни выставки было очень много посетителей, среди которых представители крупных заказчиков – компаний теплоэнергетического комплекса и силовых структур. Они обращали внимание на каждую новинку, досконально рассматривали экспозиции, подолгу общаясь с разработчиками

Состав экспонентов по сравнению с позапрошлым годом не сильно изменился, в основном присутствовали старые "зубры", не первый год принимающие участие в подобных мероприятиях.

Требуется ускорение комплексных решений

Основной тенденцией выставки, отражающей вектор движения рынка технических систем безопасности, стоит назвать проектные продажи комплексных решений. Иными словами, это означает, что производитель должен учитывать различные точки зрения на свой продукт, начиная от заказчика и далее по цепочке: проектировщик, лицо, осуществляющее закупки, монтажник и, наконец, эксплуатант.

Если этого не сделать, то продукт, скорее всего, на каком-то из этапов "замерзнет" и не выйдет на рынок. А если даже и выйдет, то продаваться успешно не будет. Такой длительный, измеряемый годами процесс подразумевает четко просчитанную стратегию, от разработки до введения в эксплуатацию.

Компании, которые придерживаются такого принципа, годами совершенствуют свою структуру и опыт. Они имеют тесный контакт со всеми представителями вышеуказанных групп на рынке, поэтому могут успешно конкурировать и продвигать свои продукты или услуги. Личное общение на выставке Securika с поставщиками, заказчиками, проектировщиками лишний раз подтвердило это.

Процесс может быть ускорен, если производитель изначально хорошо ориентируется в проблемах и задачах каждого участника рынка. Ошибки в стратегии продвижения продукции на рынке неминуемо приведут к плачевному результату.

Продукт сложно и долго выходит на рынок, тем более если это не единичное изделие, а комплекс. В этом случае и подход нужен комплексный.

Технические решения в комплексах должны учитывать тенденции развития и изменения конъюнктуры на несколько лет вперед, а это очень непросто! Рынок же сегодня требует быстрого, простого и малобюджетного решения.

Эти противоречивые требования, как лебедь, рак и щука, сегодня буквально разрывают реального производителя, производителя без всяких кавычек, который не гонит контрафакт, не дает "откаты", да еще платит все налоги!

Но другого выхода нет – жестокая борьба с коррупцией постепенно освобождает рынок от горе-производителей и горе-заказчиков!

Необходимы единые нормы и стандарты

Реализовать на объекте современный охранный комплекс довольно сложно еще и потому, что в работе почти всегда участвует не одна, а несколько компаний.

При этом те, кто создает комплексы, должны учитывать возможность других компаний интегрировать свои продукты в их технические решения, тем более что единого подхода к тактике охраны не существует. Технические задания разрознены: у каждого заказчика свои отраслевые требования. Безусловно, должны быть какие-то ориентиры на единые нормы или стандарты, но это уже отдельная больная тема. К примеру, пресловутый ГОСТ на единые технические требования к противотаранным устройствам уже несколько лет никак не может вступить в силу, хотя разработчиками он уже давно подготовлен! Процедура его принятия Росстандартом проходит крайне медленно, с постоянными ссылками на "объективные трудности".

Производитель должен учитывать различные точки зрения на свой продукт, начиная от заказчика и далее по цепочке: проектировщик, лицо, осуществляющее закупки, монтажник и, наконец, эксплуатант. Если этого не сделать, то продукт, скорее всего, на каком-то из этапов "замерзнет" и не выйдет на рынок. А если даже и выйдет, то продаваться успешно не будет



www.rocknrollaudiovideo.com

Технические решения в комплексных проектах должны учитывать тенденции развития и изменения конъюнктуры на несколько лет вперед. Рынок сегодня требует быстрого, простого и малобюджетного решения

В отсутствие таких стандартов рынок зачастую опирается исключительно на цену, а не на объективные, подтвержденные натурными испытаниями характеристики. Увы, но именно цену, а не качество сегодня ставят во главу угла!

Конечно, рынка без проблем и острых вопросов не бывает, как в любых развивающихся системах или организмах. Будем же надеяться и верить в то, что выигрыш все-таки достанется настоящему отечественному производителю! ■

Виталий Кобзун

Редактор раздела "Комплексная безопасность", генеральный директор ООО "Радиорубеж"

Робототехнические технологии для минимизации последствий аварий и катастроф на критически важных объектах

Станислав Симанов
Старший научный сотрудник ФГБУ ВНИИПО МЧС России

В стратегии национальной безопасности, которая изложена в Указе Президента РФ от 31 декабря 2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации", сформированы стратегические национальные приоритеты, одним из которых на уровне обороны страны является государственная и общественная безопасность. К основным угрозам государственной и общественной безопасности относятся стихийные бедствия, аварии и катастрофы, связанные в том числе с глобальными изменениями климата

Последствия таких чрезвычайных ситуаций могут значительно возрасти при нарушении нормальных условий функционирования ряда объектов экономики. Для того чтобы систематизировать объекты, на которых нужно сосредоточить особое внимание с точки зрения государственной и общественной безопасности, была разработана методика отнесения объектов к критически важным. Как правило, они защищаются специальным подразделением Федеральной противопожарной службы МЧС России. Именно о таких объектах и пойдет речь далее.







Рис. 1. Аварии на критически важных объектах

Ликвидация аварий и их последствий на критически важных объектах

Когда на критически важном объекте происходит авария (или катастрофа), запускаются в работу план ее ликвидации и используются соответствующие технические решения, включая робототехнические комплексы (РТК). Самыми сложными объектами ликвидации аварий считаются ядерно и радиационно опасные объекты экономики (рис. 1).

Первое массовое применение робототехники на Чернобыльской АЭС (рис. 2) показало ее высокую эффективность при правильной ее эксплуатации и оперативно принятых верных решений. В 1997 г. в Арзамасе-16 произошла менее серьезная по масштабам авария, но она также потребовала принятия решений по применению робототехники (по опыту ликвидации аварии на ЧАЭС).

1997 год, по сути, стал "точкой отсчета" в системе МЧС, когда начала развиваться робототехника специального назначения, предназначенная для ликвидации последствий ЧС. С тех пор изменилось только ее технологическое оснащение, сам принцип применения остался тот же.



Рис. 2. Применение робототехники для ликвидации последствий аварии на Чернобыльской АЭС (СССР, 1986 г.)

Указом Президента РФ от 16 декабря 2015 г. № 623 "О Национальном центре развития технологий и базовых элементов робототехники" робототехника была признана в России одним из приоритетных направлений развития науки и технологий наравне с безопасностью, противодействием терроризму и т.д.

В 2016 г. приказом МЧС России № 39 за ФГБУ ВНИИПО МЧС России была закреплена роль головного учреждения, отвечающего за стратегию развития робототехники, ее внедрения и применения в системе МЧС.

Технологии ликвидации аварий и их последствий на потенциально опасных объектах

Минимизация ущерба критически важным объектам от последствий аварий и катастроф – это комплексная организационно-техническая задача, направленная на эффективное реагирование в ходе проведения аварийно-спасательных и других неотложных работ (АСДНР). Основными показателями эффективности являются:

- максимальное снижение риска травмирования (гибели) личного состава ликвидаторов при проведении АСДНР;
- оперативное, своевременное и правильное принятие решений на АСДНР (по организации работ, выделению необходимого и достаточного количества сил и средств, материальных ресурсов и т.д.);
- снижение общего времени ликвидации аварий и катастроф за счет применения современных аварийно-спасательных технологий, техники и оборудования, материальных средств и т.д.





Рис. 3. Применение робототехники для ликвидации последствий аварии на АЭС "Фукусима" (Япония, 2011 г.)





Рис. 4. Арсенал Минобороны России (2011 г.)









Рис. 5. Полигон в Московской области для отработки технологий (сверху – реальное предприятие, внизу слева – полный 3D-план, внизу справа – версия, полученная с помощью лазерного сканера)

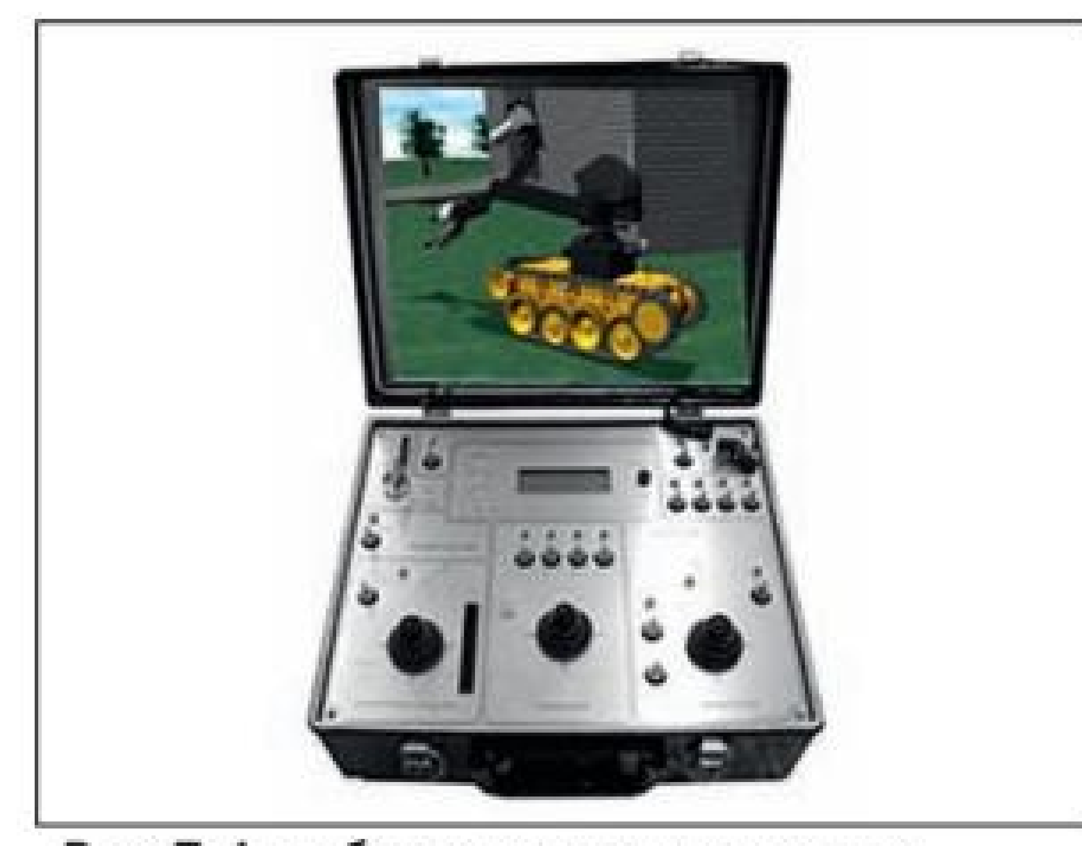


Рис. 7. Апробация смоделированных аварийных ситуаций



Рис. 8. Филиал ФГБУ ВНИИПО МЧС России в Оренбурге





Рис. 6. 3D-план цехов помогает смоделировать маршрут движения применяемых роботизированных аварийных средств

В основе современных и перспективных аварийно-спасательных технологий лежат базовые принципы Индустрии 4.0, а именно технология создания "цифровых близнецов" (Digital Twins).

Моделирование аварийных ситуаций

На рис. 5 изображены действующий объект и его "двойник", расположенный на полигоне МЧС России, находящемся в Московской области, и представляет собой разрушенный цех химического предприятия. На территории полигона созданы, отработаны и представлены различные проектные решения, использующиеся сегодня в сфере электроэнергетики, метрополитена, нефтегазового сектора и т.д.

Главная особенность и преимущество способа моделирования аварийных ситуаций при получении достоверной и реалистичной 3D-модели защищаемого КВО – применение не только графических систем САПР, но и технологий физической съемки лазерным сканером. С помощью лазерного сканера можно снять реальную обстановку, чтобы затем на "двойнике" объекта отрабатывать различные тактические приемы в комплексе с техническими решениями по проведению аварийно-спасательных работ и т.д.

3D-план цехов и самого предприятия, как правило, разрабатывается в процессе построения и ввода в эксплуатацию всего сооружения или объекта в целом. Например, на рис. 6 показан участок цеха, в котором произошла авария. В случае разрушения каких-либо конструкций туда не отправляются люди – достаточно применения лазерного сканера, который может работать на удалении до 1 км. "Снимок", полученный с места аварии, накладывается на имеющийся 3D-план, что позволяет:

- понять, какое именно оборудование на объекте попало в сектор аварии;
- принимать адекватные решения, не заходя в опасную зону аварии;
- смоделировать маршрут движения применяемых роботизированных аварийных средств.

Робототехнические комплексы не только оснащены специальным техническим оборудованием для аварийно-спасательных работ, но и доставляют в очаг поражения и развития ЧС датчики, с которых в режиме реального времени можно получать самую оперативную и достоверную информацию.

Отработка на тренажерах

Моделирование аварийных ситуаций на первичном этапе целесообразно отрабатывать на тренажерах. При этом нужно понимать, что тренажер пульта управления должен соответствовать реальному пульту управления того робототехнического комплекса или системы, которые находятся на конкретном предприятии, а на полигоне уже отрабатывать практические нюансы, связанные с выполнением этих задач.

Самый главный показатель эффективности ликвидации аварии, при выполнении аварийно-спасательных работ, – это время. Чем короче время ликвидации ЧС, тем меньший ущерб будет нанесен объекту экономики (особо охраняемой территории).

Внедрение инновационных технологий

На территории филиала ФГБУ ВНИИПО МЧС России в Оренбурге возведен роботодром для проведения опытной эксплуатации и полигонных испытаний перспективных образцов РТК и специализированной пожарной и аварийно-спасательной техники.

Испытания робототехники проводятся на следующих объектах полигона:

- резервуарный парк с резервуарами определенных типоразмеров;
- газонефтяная технологическая площадка;
- объекты малотоннажного хранения СПГ.

Создание центра огневой подготовки и аттестации пожарных и аварийно-спасательных формирований различных категорий, соответствующего требованиям международной классификации, – ближайшая задача.

Одно из основных направлений работы филиала на данный момент – аккредитация полигонной базы в ведущих международных центрах противопожарной защиты как площадки для исследования и оценки средств и способов борьбы с пожарами. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Статья опубликована в каталоге "Пожарная безопасность", 2021 г.

Рынок охранных услуг. Охранный мониторинг. ПО для охранных предприятий

Мнения экспертов

Основные проблемы охранных предприятий – это кадровый голод, особенно в регионах, слабый уровень маркетинга и зачастую полное отсутствие стратегии и инструментов по продвижению своих услуг и привлечению клиентов. Более 60% охранных предприятий не имеют собственного сайта, при этом 80% потребителей ищут поставщиков данных услуг именно через Интернет



Юрий Михайлов
Директор
ООО "Крипто Групп"



Андрей Степанов
Начальник отдела маркетинга
Охранного бюро "СОКРАТ"



Андрей Демидюк
Научный руководитель – заместитель генерального директора ООО "Рубеж-Инжиниринг", д.в.н., профессор, действительный член Академии военных наук



Алексей Бахмутов
Руководитель проектов систем безопасности
ООО "Альтоника СБ"

В каких сферах услуги охранных предприятий являются наиболее востребованными?

Юрий Михайлов, "Крипто Групп"

Если говорить о пультовой охране и защите объектов техническими средствами охраны, не принимая во внимание рынок физической охраны, то наиболее востребованными услуги охранных предприятий остаются в секторе малого и среднего бизнеса, а также в "квартирном" сегменте. Основными потребителями услуг частных охранных организаций (ЧОО) являются микропредприятия и частные лица, которые в условиях жесткой конкурентной борьбы между охранными компаниями могут подобрать поставщика охранных услуг за приемлемые деньги. Статистика поисковых запросов в Яндексе показывает, что установка систем видеонаблюдения и охранной сигнализации в квартиру, дом, гараж – наиболее востребованные услуги на рынке охраны частной собственности. Наиболее популярные запросы от предприятий малого бизнеса – установка охранно-пожарной сигнализации, тревожной кнопки и видеонаблюдения. Для этих обеих групп потребителей запросы на перечисленные услуги охраны обусловлены рисками, которым они подвержены, и по своему характеру эти риски схожи.

Андрей Степанов, "СОКРАТ"

Наиболее развивающийся сейчас сектор, который пользуется услугами охранных предприятий, – это частный сектор. В последнее время растет количество семей, которые предпочитают направлять материальные средства на строительство дома, а не покупки квартиры в МКД. Данный рынок сейчас развивается, и пандемия, как ни странно, также способствует стремлению людей заиметь загородный жилой дом. И конечно же, оставлять его без охраны – чистой воды безрассудство. Поставить дом на охрану – одна из первостепенных задач, которая встает перед новоселами.

Андрей Демидюк, "Рубеж-Инжиниринг"

Угрозы противоправных действий будут смещаться в область высокотехнологичных средств и способов их совершения. Одними из наиболее опасных могут быть способы нанесения ущерба жизни, здоровью людей, их имуществу и имущественному фонду организаций или их конфиденциальности, связанные с применением беспилотных авиационных средств. Доступность и широкое распространение таких средств, в особенности миниатюрных классов, и несовершенство законодательной базы делает угрозы их применения актуальными, а услуги охранных организаций по противодействию этим угрозам – востребованными.

Алексей Бахмутов, "Альтоника СБ"

На мой взгляд, услуги охранных предприятий являются наиболее востребованными в торговой сфере, по причине большого количества открывающихся ТЦ, рынков и тому подобных объектов по всей территории РФ, где необходимо обеспечить безопасность граждан. Особенно это актуально в условиях распространения коронавирусной инфекции. Услуги охранных предприятий также являются и будут наиболее востребованными в ближайшие годы в сфере ЖКХ, а именно в охране физическими лицами своего жилья и имущества. Данная востребованность будет связана прежде всего с программой реновации. При получении нового жилья собственник захочет обеспечить его защиту от злоумышленников, тем самым он будет подключаться к пультовой охране.

С какими трудностями в настоящее время сталкиваются охранные организации в России?

Услуги охранных предприятий являются наиболее востребованными в торговой сфере, по причине большого количества открывающихся ТЦ, рынков и тому подобных объектов по всей территории РФ, где необходимо обеспечить безопасность граждан

Юрий Михайлов, "Крипто Групп"

Не хочу затрагивать избитую тему с эпидемией коронавирусной инфекции, последствия пандемии отразились на всех сферах деятельности, и ЧОП тут не исключение. К основным проблемам многих охранных предприятий могу отнести кадровый голод, особенно в регионах, слабый уровень маркетинга и зачастую полное отсутствие стратегии и инструментов по продвижению своих услуг и привлечению клиентов. Очевидно, что эти проблемы взаимосвязаны, и обусловлены они не отсутствием профильных специалистов на рынке труда, а в первую очередь нежеланием руководителей охранных компаний повышать уровень своих компетенций, погружаться в эти бизнес-процессы или привлекать в компанию необходимых профессионалов. В подтверждение своих слов могу привести, на мой взгляд, показательные цифры. Более 60% охранных предприятий не имеют собственного сайта, при этом 80% потребителей охранных услуг ищут поставщиков данных услуг именно через Интернет.

Андрей Степанов, "СОКРАТ"

Трудности вытекают из моего предыдущего ответа – удаленность охраняемых объектов от центра охраны и необходимость содержания минимально необходимого количества экипажей групп быстрого реагирования (ГБР). Также современный потребитель достаточно избалован и уже давно забыл, что такое дефицит услуг и товаров. Конечно же, это хорошо, когда есть из чего выбрать, и услуги охранных предприятий здесь тоже не исключение. Поэтому тот, кто сможет предложить больше опций за минимальную цену, сможет укрепиться на рынке охранных услуг или даже расширить свою часть рынка.

Андрей Демидюк, "Рубеж-Инжиниринг"

В рамках задачи противодействия противоправному применению миниатюрных беспилотных летательных аппаратов (мини-БПЛА), как и других высокотехнологичных угроз, основные трудности состоят в недостаточной технической оснащенности охранных организаций и подготовленности их персонала для эффективного применения современных средств контроля и противодействия таким угрозам. Эти трудности являются следствием низкой информированности руководства таких организаций о существующих на рынке технических средствах контроля и противодействия мини-БПЛА, применение которых допустимо, например, в населенных пунктах и не несет риски для жизни и здоровья людей.

Алексей Бахмутов, "Альтоника СБ"

В настоящее время основной трудностью, с которой сталкиваются охранные организации в России, можно назвать привлечение новых клиентов. В сфере безопасности большое количество охранных организаций, оказывающих услуги охраны. Для каждой из них привлечь и удержать новых клиентов на более-менее выгодных условиях является приоритетной задачей. В условиях жесткой конкуренции идет сильный демпинг, поэтому нужно научиться договариваться и в то же время предоставлять нормальные, соответствующие требованиям клиента, услуги.

Какие тенденции существуют на рынке охранных услуг?

Показательным примером автоматизации в сфере охранных услуг являются роботизированные колл-центры, которые способны снять колоссальную нагрузку с пульта централизованного наблюдения и без участия человека предоставить клиенту информацию о состоянии охраняемого объекта, проверить с клиентом тревожную кнопку, обзвонить должников, сверить списки ответственных лиц по объекту и т.д.

Юрий Михайлов, "Крипто Групп"

За последние несколько лет главные позиции закрепили за собой тенденции, направленные на автоматизацию бизнес-процессов и развитие клиентских сервисов. Охранные компании, которые задают тренды или следуют им, занимают лидирующие позиции, используя эти инструменты как для привлечения клиентов, так и для повышения своей технологичности. Одно вытекает из другого. Согласитесь, сегодня мы уже не представляем нашу жизнь без мобильных приложений. Мы привыкли получать быстрый доступ к информации, проверять баланс телефона и оплачивать услуги через личный кабинет. Для нас является нормой следовать командам голосовых помощников при звонке на многоканальные телефоны банков или других провайдеров услуг. Эти инструменты делают нашу жизнь комфортной и обеспечивают высокий уровень сервиса, но при этом ставят перед поставщиками таких услуг задачи по цифровизации своего бизнеса и автоматизации этих процессов, ведь без этого предоставление такого рода услуг будет попросту невозможным. Показательным примером такой автоматизации в сфере охранных услуг являются роботизированные колл-центры, которые способны снять колоссальную нагрузку с пульта централизованного наблюдения (ПЦН) и без участия человека предоставить клиенту информацию о состоянии охраняемого объекта, проверить с клиентом тревожную кнопку, обзвонить должников, сверить списки ответственных лиц по объекту и т.д. Только один такой инструмент способен выполнять работу, для которой потребовалось бы два-три человека, а их содержание обошлось бы охранному предприятию около 1 млн рублей в год.

Андрей Степанов, "СОКРАТ"

Тенденция сейчас одна, и она довольно ярко выражена – видеонаблюдение. Импортные и некоторые отечественные коробочные комплекты стоят довольно недорого и позволяют хранить в облаке архив видеозаписей, имея постоянный доступ к ним через мобильное приложение. Поэтому, если вы прилагаете к услугам охраны видеонаблюдение, это предложение становится очень привлекательным, зачастую полностью нивелируя повышенную стоимость.

Андрей Демидюк, "Рубеж-Инжиниринг"

Основные тенденции на рынке охранных услуг связаны с развитием технических средств дистанционного контроля и оповещения об угрозах, а также их интеграции в единые комплексы. Ввиду этого можно предположить, что в перспективе часть функций охранных структур, связанных с применением интегрированных комплексов контроля и защиты, могут профессионально исполняться специализированными организациями на аутсорсинге. Например, можно предположить, что эффективно бороться с мини-БПЛА возможно, только объединив усилия локальных систем охраны объектов в единую сеть обмена информацией.

Алексей Бахмутов, "Альтоника СБ"

Охранные организации все большее внимание уделяют удобству и качеству получения охранной услуги клиентом. В частности, они разрабатывают всевозможные приложения, в которых клиент может в режиме реального времени видеть, что происходит на объекте, может включить/выключить свет или, скажем, удаленно сам поставить/снять объект с охраны, пополнить баланс и т.п. Данный функционал упрощает клиенту общение с охранной организацией и в то же время позволяет ему полноценно удаленно управлять своей системой.

Серверное ПО "Приток-Охрана-Web" для клиентов охраны и обслуживающих организаций

Представляет ОБ "СОКРАТ" www.sokrat.ru





Проекты

Подразделения УВО по РФ, МВД Узбекистана, ЧОО (ЧОП), Иркутский авиазавод, отдельные подразделения Сбербанка по РФ

Реклама

Появление на рынке	Июнь 2018 г.
Ценовой сегмент	Средний

Новый подход к решению задач

"Приток-Охрана-Web" – это дополнительное программное обеспечение, позволяющее расширить функции системы "Приток-А":

1. Возможность для пользователей контролировать состояние охраны через мобильное приложение.
2. Сбор информации с нескольких обособленных пультов мониторинга (охраны).
3. Работа с обслуживающими охранные приборы организациями через электронный журнал заявок.
4. Обеспечение интеграции с видеосистемами Axxon Next или Intellect, DOMINATION по схеме "видеокамера – мобильное приложение". Более того, "Приток-Охрана-Web" позволяет интегрировать экипажи ГБР в информационное поле охранной организации.

Инновационность

Основная концепция – предоставление клиентским приложениям безопасного и контролируемого доступа к информации по охраняемым объектам. По сути, это стена, разделяющая информационное пространство охранной организации и безграничную сеть Интернет.

ПО "Приток-Охрана-Web" можно представить как мультимедийную систему для вашего автомобиля – машина без нее поедет, но с ней гораздо интереснее!

Потребители

Промышленные и торговые предприятия с собственными СБ и разветвленной сетью филиалов, охранные и монтажные организации

Технические особенности

Неограниченное количество внешних и внутренних подключений.

Что оценят потребители

Система представлена практически по всей стране. Наши представители в регионах всегда готовы оказать помощь при запуске и поддержке. Система подходит как для небольших мониторинговых компаний, так и для крупных сетей предприятий.

Экономическая эффективность

Покупатель получает не просто охранную систему, а целый комплекс, позволяющий создать сложный, распределенный мониторинговый центр для контроля объектов независимо от их местоположения. ■

см. стр. 120 "Ньюсмейкеры"

АРМ ПЦО "Эгида-3": то, что нужно ЧОПу!

Представляет ЗАО "НВП "Болид" www.bolid.ru



Проекты

Объекты ОАО "Роснефть", объекты ОАО "Газпром" в северных регионах РФ, сеть торговых центров "Глобус" и "Ашан", международный аэропорт "Волгоград", объекты горно-добывающей промышленности (Якутия, Республика Коми), ПАО "Сбербанк России", объекты банка ВТБ, ЦССИ ФСО России в Челябинской области, Нижневартовске, месторождения нефти (АО "Томск-нефть"), АО "Мосгаз", филиалы АО "Почта России", объекты АО "РЖД", МДЦ "Артек", Ульяновский автомобильный завод, Михайловский горно-обогатительный комбинат, офисы продаж МТС, объекты АО "Роснефть", ФКП "Аэропорты Севера", компании "Группа ПИК", ГУП "Московский метрополитен", Троице-Сергиева Лавра (г. Сергиев-Посад) и др.

Реклама

Появление на рынке	Июнь 2011 г.
Ценовой сегмент	Средний

Потребители

ЧОП, управляющие компании, обслуживающие организации. Для любых объектов, подлежащих централизованной пультовой охране

Новый подход к решению задач

АРМ ПЦО "Эгида-3" обеспечивает независимость от типа канала связи передачи тревожных сообщений, интеграцию с охранным оборудованием разных производителей в единый мониторинговый центр и непрерывный мониторинг состояния оборудования на объекте.

Конкурентные преимущества

Возможность работы с разными каналами связи: GSM, радиоканал, мобильный Интернет, локальная сеть, ГТС, проводные линии RS-232/485, спутниковая связь с резервированием маршрутов передачи и каналов связи. Модульность и масштабируемость графического интерфейса рабочего места оператора. Видеоверификация тревог.

Инновационные характеристики

- Кросс-платформенный фреймворк для разработки и портирования программного обеспечения.
- Интероперабельность программного обеспечения.
- Гибридные мобильные приложения.
- Инновационные технологии видеонаблюдения.

Технические особенности

- До 10 тыс. объектов охраны.
- Поддержка 5 каналов связи.

Что оценят потребители

- Простота подключения объектов.
- Совместимость комплекса с любой охранной сигнализацией.
- Прямая интеграция с широко распространенной системой охраны ИСО "Орион".
- Бесплатные приложения для абонентов: личный кабинет, тревожная кнопка, АРМ ГБР, оповещение абонентов по СМС и электронной почте.

Экономическая эффективность

Более 10 лет производства, около 100 тыс. объектов на территории РФ. Инсталляции в странах ближнего зарубежья: Абхазии, Казахстане (Астана, Павлодар, Караганда), Киргизии (Бишкек), Монголии и др.

Бесплатные обновления и поддержка продукта. ■

см. стр. 120 "Ньюсмейкеры"

Какие современные технологии способствуют развитию охранного рынка?

Юрий Михайлов, "Крипто Групп"

В настоящее время наибольшую популярность среди заказчиков и поставщиков охранных услуг набирают технологии беспроводной передачи данных, цифровые адресные системы охранно-пожарного мониторинга, системы интеллектуального видеомониторинга. Эти технологии решают ряд важных задач, к которым можно отнести высокую скорость реализации проектов, феноменальную информативность и аккумулирование большого объема данных для аналитики и за счет этого возможность построения интеллектуальных обучаемых систем мониторинга. За этими технологиями будущее.

Андрей Степанов, "СОКРАТ"

Интернет, облачные сервисы, мобильные приложения – вот трио, которое диктует в XXI веке тенденции развития. Мобильные мессенджеры, социальные сети, домашние камеры с управлением со смартфона, умные розетки-лампы, роботы-пылесосы, голосовые помощники – это уже реальность и это уже освоенный массовый рынок. Поэтому если ваш продукт не имеет связи с этим трио технологий и не позволяет включить себя в цифровую экосистему пользователя, то это анахронизм и его ждет печальная участь.

Андрей Демидюк, "Рубеж-Инжиниринг"

Таких технологий множество, и каждая из них имеет свои достоинства и недостатки. Компенсация недостатков одних технологий достоинствами других и тем самым повышение надежности охраны объектов предполагает интеграцию таких технологий в рамках одного охранного комплекса. Например, технология контроля обстановки с использованием оптико-электронных средств имеет существенные ограничения по гидрометеорологическим условиям, времени суток и дальности наблюдения. С другой стороны, например, средства пирамидальной охраны, основанные на радиолокационных методах обнаружения, ограничены условиями распространения радиоволн и влиянием помех различного вида.

Алексей Бахмутов, "Альтоника СБ"

Все большую популярность в России получают системы видеонаблюдения. С помощью данных систем охранные организации имеют возможность зафиксировать, к примеру, такие преступления, как несанкционированное проникновение, хищение в магазине, порчу имущества и т.д. Пользуется популярностью также система распознавания лиц, которая своевременно позволяет обнаружить злоумышленника, занесенного в базу, и передать информацию в охранную организацию о нем и его местоположении.

Когда можно рекомендовать заказчику пультовую охрану, а в каких случаях более приемлема охрана физическая?

Юрий Михайлов, "Крипто Групп"

Ответ очевиден: в тех случаях, когда заказчику это будет выгодно. Если речь идет об охране объектов, то пультовая охрана всегда будет предпочтительней физической. Исключением будут являться объекты, на которых нет технической возможности организовать охрану аппаратными средствами сигнализации, объекты, которые находятся на значительном удалении и где реагирование силами мобильных экипажей выходит за рамки допустимого транспортного времени, а также режимные объекты, на которые доступ экипажам ГБР ограничен. На последних проще организовать собственный пульт охраны, осуществлять патрулирование территории и реагирование силами сотрудников охраны. В остальных случаях альтернативы пультовой охране практически не существует. Причин этому несколько. Во-первых, на сегодняшний день человек не способен конкурировать с техническими средствами защиты, которые мгновенно фиксируют малейшие нарушения в охраняемых зонах. В этом смысле пультовая охрана полностью исключает человеческий фактор, а совокупность технических средств позволяет защищать объект не только от проникновений, но и от возгораний, утечек газа и протечек воды и других рисков. Во-вторых, стоимость оснащения объекта сигнализацией в итоге обойдется заказчику выгоднее, чем содержание поста физической охраны.



Андрей Степанов, "СОКРАТ"

Пультовая охрана в первую очередь предназначена для снижения стоимости охраны для массового сегмента с сохранением эффективности мероприятий по предотвращению происшествий. Другими словами, недорогой гарант безопасности для множества объектов. При этом сам факт происшествия на объекте не несет фатальных последствий для охраняемого объекта. Физическая охрана подразумевает не столько сигнализирование о происшествии, сколько применение превентивных мероприятий, в том числе нейтрализации угрозы до события, для предотвращения происшествия. Поэтому физическая охрана просто необходима на крупных промышленных предприятиях и крупных коммерческих объектах, например торговых комплексах, бизнес-центрах и т.п. При этом для промышленных предприятий вполне логичен и комбинированный подход к охране – она централизованная и физическая.

Андрей Демидюк, "Рубеж-Инжиниринг"

Выбор того или иного способа охраны определяется характеристиками объекта защиты, условиями охраны, требованиями к степени защищенности объекта (вероятность предотвращенного ущерба) и финансовыми возможностями их реализации. Так называемая пультовая охрана предполагает прежде всего более высокую техническую оснащенность средствами охраны соответствующих служб. При их недостаточности применяется физическая охрана. С другой стороны, одно должно дополнять другое. Известно, что наиболее совершенными системами охраны являются те, где резервируются не только средства, но и способы охраны.

Алексей Бахмутов, "Альтоника СБ"

В случае когда у заказчика такой объект, как магазин, киоск, коттедж и т.п., и большое количество времени он не проводит на данном объекте, лучше рекомендовать ему пультовую охрану. Данный способ позволит сэкономить на установке охранного оборудования, так как зарплата охранника в разы выше стоимости оборудования.

В случае если вам нужно обеспечить объект временной охраной (склад, завод, офис, дом и т.п.), выгоднее рекомендовать заказчику физическую охрану. Данный способ позволит сэкономить на установке охранного оборудования, а физическая охрана лишь ускорит реагирование. Для более эффективной физической охраны заказчику можно использовать технические средства охраны, которые позволят ему быть в курсе, осуществляется ли круглосуточное патрулирование охранниками его объекта или они в это время спят или смотрят телевизор.

По оценкам BusinesStat, в 2021–2025 гг. можно ждать минимального роста объема рынка охранных услуг на 1,2–2,5% в год. Согласны ли вы с этим предположением? Какие перспективы у рынка охранных услуг?

Юрий Михайлов, "Крипто Групп"

Рост рынка охранных услуг напрямую зависит от роста экономики в стране. В этом смысле можно опираться на показатели и прогнозы Минэкономразвития. Как бы это ни было грустно, но, на мой взгляд, с оценками BusinesStat можно согласиться, позитивных тенденций для роста нашей отрасли я пока что не вижу.

Андрей Степанов, "СОКРАТ"

Я бы предположил 5%-ный рост объема. Частично оттого, что на сегодня многие строительные компании ради привлечения клиентов закладывают еще на стадии проектирования различные комплексы систем безопасности, что позволяет безусловно включить в сферу обслуживания новых клиентов. Кроме этого, многие промышленные компании открывают новые объекты и начинают ставить новое оборудование или проводить модернизацию старого. Поэтому рынок охранных услуг в ближайшие несколько лет будет стабильно продолжать рост.

Андрей Демидюк, "Рубеж-Инжиниринг"

В контексте предыдущих ответов перспективой рынка охранных услуг станет увеличение доли высокотехнологичных средств и способов охраны. Это обстоятельство и необходимость обеспечить глобальную и непрерывную защиту объектов от разнохарактерных угроз потребует значительных дополнительных инвестиций в эту отрасль, что скажется на росте его объемов в будущем.

Алексей Бахмутов, "Альтоника СБ"

В связи с постоянной цифровизацией безопасности, когда злоумышленникам все сложнее совершать преступления и при этом оставаться незамеченными, а также последствиями коронавирусной инфекции (многие объекты закрылись во время пандемии) возможен минимальный рост объема рынка охранных услуг. Будем надеяться, что в ближайшем будущем не сократится строительство социальных объектов и многоквартирных домов. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Владимир Балановский
Член бюро комиссии РАН по техногенной безопасности, проф. Академии военных наук

Антон Прокопчук
Начальник центра информационных технологий связи и защиты информации ГУ МВД России по г. Москве

Нина Николаева
Программный директор международного форума "Технологии безопасности"

Кирилл Ямanов
Директор департамента по работе с государственным сектором АО НИП "Информзащита"

Леонид Балановский
Руководитель направления АО НИП "Информзащита"

Системы безопасности против современных угроз

В связи с трагедией в Казани президент РФ Владимир Путин дал правительству поручение внедрить единый подход к обеспечению безопасности и антитеррористической защищенности образовательных учреждений[1]. Рассмотрим, какой опыт и какие проблемы существуют, что нужно изменить для усиления эффективности защиты таких объектов

Совершенствование систем безопасности для эффективного противодействия комплексу современных угроз в первую очередь должно осуществляться для организаций с массовым пребыванием людей. Например, в Москве запущена программа капитального ремонта и до конца 2023 г. планируется отремонтировать 135 поликлиник[2], одновременно усилив их безопасность. Параллельно для реализации этой же цели в соответствии с Посланием Президента РФ Владимира Путина Федеральному Собранию РФ от 15.01.2020 г. осуществляется капитальный ремонт учебных заведений.

Образовательным учреждениям нужны эффективные системы безопасности

Ст. 41 ФЗ № 273 от 29 декабря 2012 г. "Об образовании в Российской Федерации" устанавливает, что охрана здоровья учащихся включает в себя в том числе и обеспечение их безопасности во время пребывания учебном заведении[3]. Осуществление деятельности образовательного учреждения в отсутствие систем безопасности может повлечь неблагоприятные последствия, связанные с причинением вреда жизни и здоровью граждан, создает опасные условия для неопределенного круга лиц, в том числе несовершеннолетних, нарушает их права и законные интересы.

В школах ранее уже были проведены прокурорские проверки на предмет уровня обеспечения безопасности[4]. При этом особое внимание уделялось наличию турникетов и тревожных кнопок. После трагедии, произошедшей в Казани, проверки возобновились.

Президент РФ Владимир Путин в связи с трагедией в Казани дал правительству поручение внедрить единый подход к обеспечению безопасности и антитеррористической защищенности образовательных учреждений[5]. В современных условиях вопрос стоит о срочной доукомплектации объектов в соответствии с едиными требованиями к безопасности. Важно подчеркнуть, что в условиях пандемии COVID-19 речь должна идти о комплексном подходе, включая санитарно-эпидемиологическую безопасность, а также и пожарную безопасность.

На основании пп. 6.1 п. 1 ст. 15 Федерального закона от 06.10.2003 г. № 131-ФЗ "Об общих принципах организации местного самоуправления в РФ" к вопросам местного значения муниципального района относится "участие в профилактике терроризма и экстремизма, в минимизации и (или) ликвидации последствий проявлений терроризма и экстремизма"[6]. Их выполнение направлено на обеспечение безопасности несовершеннолетних и сотрудников образовательного учреждения, их защиту от посягательств со стороны третьих лиц.

Проектные трудности

Объем вложений в системы безопасности определяется при реализации мероприятий и проектных решений, направленных на обеспечение защиты объектов от угроз террористического характера и несанкционированного вторжения согласно требованиям постановлений Правительства РФ (ПП). При несоблюдении требований и замене оборудования на более дешевое, но не указанное в проектной документации, утвержденной ФАУ "Главгосэкспертиза" и ГАУ города Москвы "Мосгосэкспертиза", такое действие рассматривается как нецелевое использование бюджетных средств.

Введение связанных с пандемией дополнений в ПП от 24 апреля 2020 г. № 579 "О внесении изменений в некоторые акты Правительства РФ, устанавливающие требования к антитеррористической защищенности объектов (территорий)" требует выполнения мероприятий в целях выявления и предотвращения несанкционированного проноса (провоза) и применения на объекте (территории) токсичных химикатов, отравляющих веществ и патогенных биологических агентов, в том числе при их получении посредством почтовых отправлений, для чего оборудуется карантинное хранилище для размещения обнаруженных подозрительных предметов и корреспонденции, что требует установки ранее не применявшихся видов оборудования. При этом проектные организации заинтересованы в том, чтобы по каждой позиции комплектующих существовало несколько видов оборудования. Это связано с тем, что каждый объект имеет свои особенности (пропускную способность, размеры и т.п.), которые диктуют требования, в том числе и стоимостные. В случае, когда существует только один производитель, который не сертифицировал оборудование, но установил на него запредельную цену, не представляется возможным выполнить требования законодательства. В результате на рынок выводится не та продукция, которая нужна, а та, которая есть (фирма вложила в нее существенные средства). Необходимо также решить проблему эффективности оборудования и его сертификации. Речь идет о нарушениях досмотрового и внутриобъектового режимов в связи с недоработками, которые в условиях коронавируса обернулись проблемой и для людей, и для государства.

Компьютеризированная методика стандартизированного многофакторного исследования личности (СМИЛ) позволяет оперативно выявлять особенности психики и отклонения в поведении и дает возможность профилактического выявления лиц, склонных к совершению преступлений террористической и экстремистской направленности

---

[1] Сергей Кравцов: "В ближайшее время будут подготовлены единые требования безопасности образовательных организаций". Официальный сайт Минпросвещения. 13.05.2021 г. URL: https://edu.gov.ru/press/3712/sergey-kravcov-v-blizhayshee-vremya-budut-podgotovleny-edinye-trebovaniya-bezopasnosti-obrazovatelnyh-organizaciy/

[2] Новый московский стандарт: как меняются городские поликлиники . Официальный сайт мэра Москвы. 27.02.2020. URL: https://www.mos.ru/news/item/70204073/

[3] Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 30.04.2021) "Об образовании в Российской Федерации". URL: http://www.consultant.ru/document/cons_doc_LAW_140174/48b9101fff215f3aeb122d86593a129a34d96d3c/

[4] Прокуратура нашла массовые нарушения в системе безопасности школ. Известия. 17.02.2014. URL: https://iz.ru/news/565854

[5] Сергей Кравцов: "В ближайшее время будут подготовлены единые требования безопасности образовательных организаций". Официальный сайт Минпросвещения. 13.05.2021г. URL: https://edu.gov.ru/press/3712/sergey-kravcov-v-blizhayshee-vremya-budut-podgotovleny-edinye-trebovaniya-bezopasnosti-obrazovatelnyh-organizaciy/

[6] Федеральный закон от 06.10.2003 № 131-ФЗ (ред. от 29.12.2020) "Об общих принципах организации местного самоуправления в Российской Федерации" (с изм. и доп., вступ. в силу с 23.03.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_44571/e6a140ee7503fa6bd6d0cba9469e0d03241273ad/

Таблица. Системы для реализации мероприятий и проектных решений, защиты от угроз террористического характера и несанкционированного вторжения

Технические системы (средства), направленные на обнаружение радиоактивных, взрывчатых, отравляющих веществ, оружия, боеприпасов, наркотических средств и других опасных предметов и веществ	Система охранная телевизионная Система охранного освещения (для системы охранного телевидения в ночное время) Система охранно-тревожной сигнализации (для обнаружения факта проникновения в охраняемые помещения с точным определением места и документированием информации, автоматической или ручной передачи сигналов тревоги на пульт подразделения ГУ МЧС России и дежурной части ОВД при возникновении на объекте ЧС экологического, техногенного или криминального характера). Она подключается к пультам централизованного наблюдения (ПЦН) ФГКУ УВО Росгвардии Система экстренной связи (для организации экстренной связи людей со специальными службами: службой спасения МЧС, полицией, скорой помощью и др.) Система контроля и управления доступом
Средства обнаружения радиоактивных, взрывчатых, отравляющих веществ, оружия, боеприпасов, наркотических средств, опасных предметов и веществ	Металлодетекторы Средства обнаружения паров взрывчатых и наркотических веществ (в том числе в почтовых отправлениях) Локализаторы взрыва Средства обнаружения радиоактивных материалов (для проведения досмотра на наличие радиоактивных материалов у подозрительных лиц, в транспортных средствах, грузах, в почтовых отправлениях) Средства досмотра транспортных средств
Технические системы (средства), направленные на оповещение находящихся в здании людей о ЧС	Система радиофикации Система радиофикации (для организации проводного вещания программ, передаваемых ФГУП РСВО, в том числе для информирования сотрудников охраны в помещении охраны) Система оповещения о пожаре и управления эвакуацией Система коллективного приема телевидения
Комплекс инженерно-технической укрепленности	Для обеспечения антитеррористической защищенности выполняются меры инженерно-технической укрепленности, мероприятия по усилению конструктивных элементов для противодействия несанкционированному проникновению, взлому и другим преступным посягательствам. Комплекс инженерно-технической укрепленности определен исходя из требований к: периметру и отдельным участкам объекта; конструктивным элементам инженерно-технической укрепленности объекта; стенам, перекрытиям и перегородкам; дверным конструкциям; оконным конструкциям помещений объекта; вентиляционным шахтам, коробам, люкам, дымоходам, технологическим каналам и отверстиям
Организация обеспечения информационной безопасности, исключающая несанкционированный доступ к информационным ресурсам объекта	На объекте предусмотрены специальные помещения, обеспеченные техническими средствами охранной, тревожной сигнализации и средствами инженерно-технической укрепленности для хранения и работы со служебной информацией ограниченного доступа: персональными данными, данными паспорта безопасности объекта, а для медицинских и образовательных учреждений – данными, составляющими врачебную тайну. В целях обеспечения необходимой степени антитеррористической защищенности специальных помещений для хранения и работы со служебной информацией ограниченного доступа предусмотрены специальные меры

Составляющие комплексной защиты

Согласно требованиям ПП от 2 августа 2019 г. № 1006 "Об утверждении требований к антитеррористической защищенности объектов (территорий) министерства просвещения РФ и объектов (территорий), относящихся к сфере деятельности министерства просвещения РФ, и формы паспорта безопасности этих объектов (территорий)" набор подсистем безопасности объекта определяется исходя из необходимости осуществления комплекса мер, направленных на его антитеррористическую защищенность:

а) на воспрепятствование неправомерному проникновению на объект (территорию);

б) на выявление потенциальных нарушителей установленных на объекте (территории) пропускного и внутриобъектового режимов и (или) признаков подготовки совершения террористического акта или его совершения;

в) на пресечение попыток совершения террористического акта на объекте (территории);

г) на минимизацию возможных последствий совершения террористического акта на объекте (территории) и ликвидацию угрозы его совершения;

д) на обеспечение защиты служебной информации ограниченного распространения, содержащейся в паспорте безопасности и иных документах объектов (территорий), в том числе служебной информации ограниченного распространения о принимаемых мерах по антитеррористической защищенности объектов (территорий);

е) на выявление и предотвращение несанкционированного проноса (провоза) и применения на объекте (территории) токсичных химикатов, отравляющих веществ и патогенных биологических агентов, в том числе при их получении посредством почтовых отправлений.

В таблице приведены системы для реализации мероприятий и проектных решений, защиты от угроз террористического характера и несанкционированного вторжения.

Изменение парадигмы безопасности

Анализ теракта в Казани показывает, что должна рассматриваться новая парадигма безопасности. Мы должны перейти от обеспечения пропускного и внутриобъектового режимов (в чем накоплен большой опыт) к обеспечению безопасности прилегающих территорий общего пользования, которыми пользуется неограниченный круг лиц. Возникает требование по созданию технологий дистанционного выявления несанкционированного вторжения. Необходима выработка единого (типового) технического решения комплексной системы безопасности учебных заведений на основе отечественного программного продукта и поправки в руководящие документы. Должны быть внесены изменения в ПП № 1006 от 2 августа 2019 г. "Об утверждении требований к антитеррористической защищенности объектов (территорий) министерства просвещения РФ и объектов (территорий), относящихся к сфере деятельности министерства просвещения РФ, и формы паспорта безопасности этих объектов (территорий)". П. 20 пп. "д" нужно изложить в следующей редакции: "исключение фактов бесконтрольного пребывания посторонних лиц и транспортных средств на объектах (территориях) или в непосредственной близости от них".

С целью повышения эффективности выполнения требований по организации и обеспечения пропускного и внутриобъектового режимов необходимо введение контроля за состоянием учащихся с помощью компьютеризированной методики стандартизированного многофакторного исследования личности (СМИЛ), позволяющей оперативно выявлять особенности их личности и отклоняющееся поведение, а также дающей возможность профилактического выявления лиц, склонных к совершению преступлений террористической и экстремистской направленности. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Как прервать цепочку событий от угрозы до происшествия и обеспечить безопасность 24/7

Все, кто занимается безопасностью в любом ее проявлении, рано или поздно сталкиваются с вопросом о способности обеспечить 100%-ную безопасность в компании. Чаще всего его задает кто-то из руководства, нередко прилюдно, ожидая четкого и однозначного ответа. Если ответить отрицательно, то потребности профильного подразделения могут сразу потерять актуальность на многие годы. Зачем давать деньги тем, кто не может обеспечить безопасность 24/7? Если же ответить утвердительно, то после уточнения, какой бюджет для этого необходим, небольшого секвестирования, процедуры согласования и реализации нужно нести персональную ответственность за все возможные инциденты. Куда ни кинь – всюду клин...

Дмитрий Дудко
Руководитель отдела проектирования и внедрения департамента информационной безопасности компании "ЛАНИТ"



Как предотвратить реализацию инцидента и приблизиться к заветным цифрам обеспечения безопасности 24/7? Для этого необходимо определиться с ключевыми элементами данной цепочки.

Активы

Те из нас, кто работает в компаниях, выделяющих значительные суммы на безопасность, могут попробовать защитить все активы. Остальным же в первую очередь нужно провести инвентаризацию объектов защиты. Каждый телефон и компьютер учитывать необязательно, важно хотя бы выделить секторы.

После проведения инвентаризации следует провести ранжирование объектов защиты. Самый наглядный, но трудоемкий способ – по финансовому ущербу. Например, если у компании украдут список клиентов, то ущерб составит 100 млн рублей, а если колесо со склада – то 20 тыс. рублей.

В качестве альтернативы можно использовать любые критерии: влияние на бизнес-процессы, величину простоя в днях, восполнимость актива, частоту использования и многое другое.

После ранжирования необходимо сделать отсечку, какие активы защищать всеми силами, а какие – "как получится". Например, все, что дороже 1 млн рублей, должно быть защищено.

Угрозы

Здесь и далее мы будем ставить знак равенства между угрозой и риском.

Классическое определение гласит: риск (от лат. resecō – "отсекать", "сокращать" или др.-греч. ῥιζικόν – "опасность") – это сочетание вероятности и последствий наступления неблагоприятных событий. А его формулу записывают так: величина риска = вероятность события х размер ущерба.

Таким образом, под угрозой мы понимаем вероятностные действия, причиняющие ущерб объектам защиты.

Предотвращение инцидентов – комплексная задача, имеющая более низкий КПД. Здесь нет универсальных рецептов, так как основной источник проблем – люди, а, как известно, человеческая душа – потемки, по крайней мере, пока службы безопасности не станут массово брать на работу телепатов

Зная активы, можно составить карту угроз для каждого из них (табл. 1).

На данном этапе не требуется составлять подробную карту угроз. Достаточно понимать основные методы воздействия на актив.

Угрозы можно разделить на два больших класса:

1) антропогенные (реализуемые человеком);

2) неантропогенные (реализуемые без участия человека).

С неантропогенными угрозами все более или менее понятно: сюда относятся стихийные бедствия, техногенные аварии, случайности. С антропогенными все несколько сложнее, так как в них появляется переменная величина – злоумышленник. Существует большая и развернутая теория классификации злоумышленников, их типов и видов. Для нашей цели достаточно понимать мотивы злоумышленника:

- финансовый интерес;
- межличностные интересы;
- доминантность.

К первой категории относятся 95% потенциальных нарушений. Мир преступлений (а особенно киберпреступлений) прагматичен: если из определенного действия нельзя извлечь материальную выгоду, то найдется очень мало желающих этим заниматься.

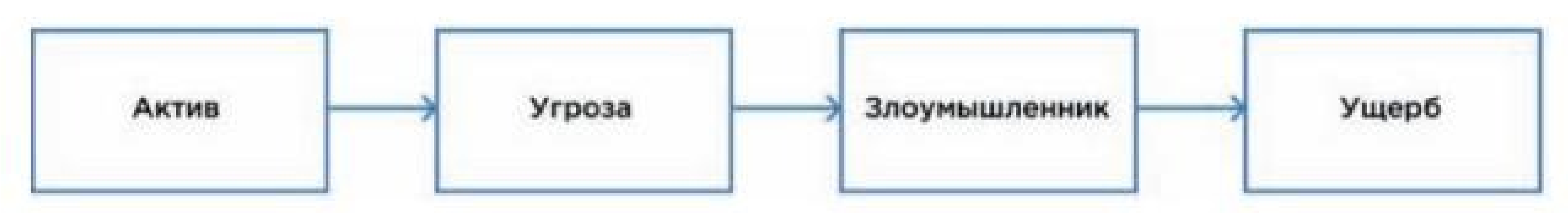


Рис. Цепочка событий от угрозы до ущерба

Таблица 1. Пример карты угроз для активов

База клиентов	Несанкционированное копирование
	Несвоевременное наполнение
Комплект колес	Кража

Таблица 2. Пример карты угроз для активов с возможными нарушителями и размером ущерба

Объект воздействия	Нарушитель	Действие	Ущерб в руб.
База клиентов	Администраторы	Несанкционированное копирование	5 000 000
База клиентов	Отдел продаж	Несвоевременное наполнение	50 000 000
Комплект колес	Кладовщик	Кража	10 000

Ко второй категории относятся все случаи слежки, например, чтобы добиться внимания женщины или отомстить обидчику.

"Вершиной" мотивов является доминирование, когда те или иные действия совершаются "просто потому, что я могу", например, обесточивание целого здания.

Определившись с нарушителями, мы можем дополнить карту угроз (табл. 2).

Таким образом, мы точно знаем цепочку событий от угрозы до инцидента (см. рис.). Теперь давайте разберемся с тем, как ее прервать.



К мотивации "финансовый интерес" можно отнести 95% потенциальных нарушений. Мир преступлений, а особенно киберпреступлений, прагматичен: если из определенного действия нельзя извлечь материальную выгоду, то найдется очень мало желающих этим заниматься

Обнаружение

В цепочке ключевым является последний пункт – ущерб. То есть инциденты, приводящие к финансовым потерям, должны обнаруживаться и предотвращаться. Обнаруживаться также должны все неудачные попытки причинить ущерб, а именно свершенные угрозы, которые не нанесли ущерба по каким-либо причинам.

Для обнаружения инцидентов необходимо выполнить ряд шагов:

1. Заручиться поддержкой высшего руководства. Без осознания возможных потерь от ущерба и требуемых мер все дальнейшие действия будут являться полумерами или полностью провалятся. При общении с топ-менеджментом выгоднее всего опираться на финансовые показали[1].
2. Понимать, знать и закрепить нормальное (обычное) состояние актива. Если колеса должны лежать на складе, то в секции Е-21. Если база клиентов располагается в общей информационной сети, то доступ к ней должны иметь отдел продаж, бухгалтерия, ИТ-администраторы и безопасники.
3. Принять меры физической защиты актива. Меры физической защиты должны зависеть от ценности актива и угроз. Колеса можно положить в секцию Е-21 под замок, выдавать ключ под роспись и поставить видеонаблюдение.
4. Принять организационные меры по защите актива. Должны быть приняты внутренние правила и регламенты по использованию актива, предоставлению доступа, списанию и уничтожению и другим применимым действиям.
5. Создать или дополнить штат службы безопасности необходимыми специалистами. Какие бы средства автоматизации вы ни применяли, при недоборе в штатном расписании вы физически не сможете вовремя реагировать на инциденты.

Получив необходимые рычаги, можно перейти к выстраиванию системы обнаружения инцидентов. Главный принцип обнаружения инцидентов – выявление отклонений от нормального состояния актива. Для этого могут использоваться различные методы и их комбинации:

1. Штатное очное наблюдение. Если ваши ресурсы позволяют поставить возле каждого ценного актива охранника с пистолетом, то необходимо этим воспользоваться. Или хотя бы разделить объект на контролируемые зоны и назначить ответственного за каждую из них.
2. Автоматизированные датчики контроля состояния актива и пространства вокруг него в зависимости от его природы. Например, при обеспечении безопасности особенно ценных материальных активов хорошо себя показывает связка датчиков движения с видеонаблюдением или СКУД. Для перемещаемых активов можно использовать RFID-метки, которые позволят не только быстро найти актив, но и следить за его перемещением.
3. Автоматизированные системы для наблюдения за контролируемыми зонами. Сюда относятся системы контроля пересечения периметра, видеонаблюдение, системы контроля доступа и т.д.
4. Для информационных систем необходимы системы мониторинга и контроля пользователей. Сюда относятся средства защиты от несанкционированного доступа, системы защиты от утечек информации (DLP-системы).
5. Для объединения всех используемых методов крайне желательно создать ситуационный центр безопасности, куда будут подключены все системы обнаружения и безопасности. Это позволит штатному составу службы безопасности работать с уже обработанной информацией, а не искать признаки инцидентов, тратя большое количество человеко-часов.

Предотвращение

Когда процессы обнаружения более или менее выстроены, перед службой безопасности часто встает задача предотвращать инциденты на ранней стадии, а не разбираться с их последствиями, то есть "бить по хвостам".

Предотвращение инцидентов – комплексная задача, имеющая более низкий КПД. Здесь нет универсальных рецептов, так как основной источник проблем – люди, а, как известно, человеческая душа – потемки, по крайней мере, пока службы безопасности не станут массово брать на работу телепатов. Здесь можно расставить лишь ориентиры для последующих действий:

1. Первое направление – это работа с сотрудниками. Сотрудники должны быть ознакомлены, желательно под подпись, с действующим режимом работы (что делать нельзя, какая ответственность за это наступает). Для подавляющего большинства людей страх наказания выше, чем сиюминутная прибыль. Там, где возможно, следует вводить материальную и коллективную ответственность, чтобы контроль и пресечение инцидентов осуществлялись коллективом.
2. Необходимо выявлять потенциально опасных сотрудников. Кто-то недоволен текущим положением, кто-то хочет уйти к конкурентам, кто-то слишком разговорчив в Интернете. Конечно, слишком сложно и дорого отслеживать каждого сотрудника, но для ключевых позиций это жизненно необходимо.
3. Важно создать комплексную скоринговую модель каждого бизнес-процесса, где участвуют ключевые активы, и занести ее в информационную систему ситуационного центра. В зависимости от приоритетов и оценок это позволит выявлять пограничные состояния перед инцидентом, когда он еще не реализовался, но вот-вот может.

Расследование

Говоря об инцидентах, нельзя обойти вниманием вопрос об их расследовании.

Расследование можно разделить на:

- внутреннее;
- с привлечением правоохранительных органов.

Разница между ними в последствиях: при внутреннем расследовании максимум, чего можно добиться, – увольнения нарушителя и иногда возмещения вреда.

Если руководство ставит задачу максимального наказания нарушителей, вплоть до привлечения к уголовной ответственности, то весь процесс обнаружения инцидентов должен быть выстроен с учетом этой особенности. Оперативно-розыскные мероприятия очень чувствительны к обстоятельствам обнаружения инцидента, сбору доказательств и свидетельских показаний. Особенно это касается инцидентов в информационных системах. Если перед вами стоит задача максимального наказания нарушителей, лучше сразу обратиться в специализированную организацию.

Главный вывод

Таким образом, к работе по обнаружению и предотвращению инцидентов следует подходить комплексно. Чем основательнее будут проведены первые этапы инвентаризации и категорирования активов и угроз, тем проще будет подобрать эффективный набор мер даже в условиях ограниченного бюджета. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

[1] Дудко Д. Вопросы совокупной стоимости владения и эксплуатации комплексных систем безопасности // Системы безопасности. 2021. № 1. С. 120–121.

Владимир Балановский
Член бюро комиссии РАН
по техногенной безопасности,
проф. Академии военных наук

Антон Прокопчук
Начальник центра информационных
технологий связи и защиты информации
ГУ МВД России по г. Москве

Алексей Авдонов
Генеральный директор
"Интерправо Инвест"

Леонид Балановский
Руководитель подразделения
ГАУ "МосжилНИИпроект"

Управление качеством безопасности объектов инфраструктуры

В настоящее время в условиях гибридной войны меняется понятие мобилизации, которая становится совокупностью мероприятий, проводимых государством для сосредоточения и приведения в активное состояние имеющихся сил, ресурсов и средств ввиду чрезвычайных обстоятельств. Источниками опасностей являются естественные процессы и явления, человеческие действия, которые таят в себе угрозу опасности. Наиболее вероятно воздействие 20 факторов: природных и техногенных, актов незаконного вмешательства (АНВ), человеческого фактора и культуры безопасности

Опыт показывает, что АНВ проводятся массированно по нескольким направлениям по типу "домино" с использованием различных методов. Отсутствие адекватных мер противодействия не позволяет обеспечивать надлежащий уровень безопасности критически важных объектов, мест массового пребывания людей и кластеров, их объединяющих.

Проблема разобщенности действий и систем

Противодействие разным видам опасностей осуществляется, в частности, на территории объектов транспортной инфраструктуры (ОТИ) различными ведомствами разобщенно, преследуя ведомственные интересы для снижения степени ответственности. Складываются параллельно функционирующие системы, что исключает возможность совместной подготовки и принятия решений по противодействию воздействиям различной природы в режиме реального времени. Суммарная стоимость таких систем безопасности с ведомственными ситуационными центрами на порядок дороже комплексной системы. Но безопасность не функция отдельной системы безопасности, а способность ОТИ в целом одинаково устойчиво работать в штатных условиях и при деструктивных воздействиях.

Формирование комплексной безопасности должно базироваться на управлении качеством с его синергическим эффектом.

Цели и задачи управления качеством безопасности

Управление качеством безопасности – это подход к управлению ОТИ, нацеленный на соблюдение нормативно заданного уровня безопасности (качества безопасности), основанный на участии всего персонала ОТИ и использовании инженерных средств, инженерно-технических систем, аппаратно-программных комплексов и направленный на достижение успеха посредством удовлетворения нормативных требований и выгоды для персонала ОТИ. Под управлением качеством безопасности понимается не только реализация безопасности как услуги, а консолидация ресурсов ОТИ в области безопасности. Внедрение повышения качества безопасности требует изменения культуры безопасности как одного из основных компонентов, определяющего уровень безопасности.

Цель управления качеством безопасности – оптимизация уровня и состояния качества безопасности с учетом экономических интересов ОТИ, а также требований устойчивого развития и непрерывности бизнеса.

Схема управления качеством безопасности ОТИ представлена на рис. 1.

Условия обеспечения качества безопасности ОТИ

Работа ведется на критических элементах ОТИ, АНВ в отношении которых приведет к полному или частичному прекращению их функционирования и (или) возникновению ЧС. Переход от "сплошной" защиты ОТИ



Рис. 1. Управление качеством безопасности ОТИ

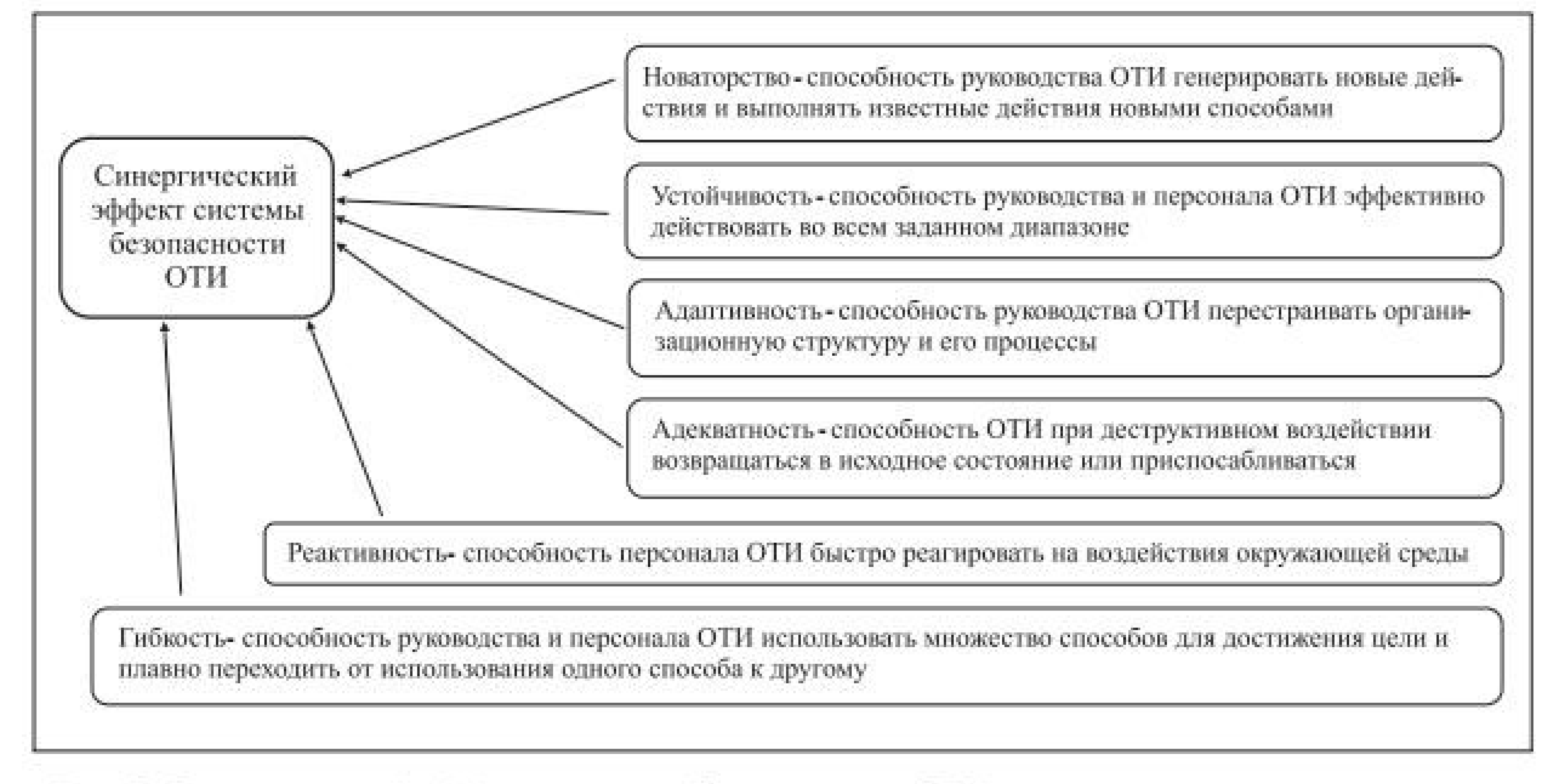


Рис. 2. Синергический эффект системы безопасности ОТИ

Таблица. Управление качеством систем безопасности ОТИ

Разработка методологии определения производственно-экономического уровня СБ ОТИ, позволяющей прогнозировать динамику развития систем безопасности и сформировать требования к ним
Разработка методологии оптимизации структуры и параметров СБ, позволяющей вырабатывать решения в интересах всего процесса создания СБ за счет согласования экономических и технических показателей качества на всех этапах жизненного цикла ОТИ
Разработка методологии структурного и параметрического синтеза, обеспечивающей оптимизацию различных вариантов межблочного комплексирования высокоэффективных СБ ОТИ и минимизацию затрат на их производство
Разработка методик расчета, анализа и оптимизации стоимостных и конструктивных параметров, показателей качества перспективных СБ ОТИ для автоматизированного решения задач синтеза и оптимизации их структуры
Разработка методики структурной и параметрической оптимизации СБ ОТИ на основе дискретного программирования, ранжирования фиксируемых и управляемых параметров, эвристического направленного перебора, интерактивного режима обработки
Разработка принципов построения программного обеспечения для синтеза перспективных СБ ОТИ с учетом оптимизации их структуры, повышения экономической эффективности, технического уровня, качества разработки и производства

На территории объектов транспортной инфраструктуры противодействие различным видам опасностей осуществляется разными ведомствами разобщенно. В результате складываются параллельно функционирующие системы, что исключает возможность совместной подготовки и принятия решений в режиме реального времени

к защите их критических элементов и внедрению управления качеством безопасности уменьшает вложения в безопасность и сокращает сроки их защиты. Происходит интеграция технических средств и организационных мероприятий в единый комплекс, автоматизация цикла реагирования на угрозы от обнаружения до ликвидации, что обеспечивает прозрачность ситуации в реальном времени.

Анализ позволяет наметить комплексы работ для оптимизации процесса разработки систем безопасности и в результате получить синергический эффект и улучшить производственно-экономические показатели. Это дает возможность надежно парировать воздействия на ОТИ факторов различной природы, значительно повысить способность локализовать последствия ЧС и ликвидировать их. Использование для оптимизации уровня безопасности ОТИ методов управления качеством безопасности с использованием методологии управления качеством позволяет получить синергический эффект, который достигается при комбинации признаков, представленных на рис. 2.

В условиях гибридной войны ключевым направлением становится создание эффективных методов синтеза СБ ОТИ. Основные этапы этой работы представлены в таблице.

Техническая и экономическая эффективность

Создание СБ на основе управления качеством безопасности должно осуществляться совместно с использованием лучших практик, наилучших доступных технологий (НДТ), энергосберегающих решений. В этом случае СБ ОТИ из планово убыточной можно превратить в экономически выгодную систему. Такой подход позволит существенно повысить эффективность обеспечения безопасности не только транспортного комплекса, но и городского хозяйства в целом, информационных технологий связи и защиты информации. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru



Опасность и безопасность транспорта

В этой статье порассуждаем о достоинствах и недостатках современного общественного транспорта. Вокруг действует целая система обеспечения безопасности, которая включает в себя одни меры со стороны государства, другие – со стороны перевозчика. Установленные правила поведения для пассажиров могут быть направлены на антитеррористическую защищенность объекта или транспортного средства, улучшение текущей санитарно-эпидемиологической обстановки либо могут быть обусловлены какими-либо иными стандартами. Однако принятие всех мер со стороны государства, перевозчика и конкретного должностного лица не может гарантировать абсолютную безопасность общественного транспорта, а порой несет в себе еще большую опасность для пассажира. Рассмотрим факторы опасности и безопасности современного транспорта и вектор развития данного направления

Иван Тушко
Специалист-эксперт в области обеспечения транспортной безопасности, магистр юриспруденции

Транспорт играет огромную роль в жизни любого современного человека и занимает особое место в развитии инфраструктуры города и целого государства. Так как транспортный комплекс крайне важен для экономической деятельности любой страны, то неотъемлемым требованием к транспортной инфраструктуре является способность противостоять любым видам внешних угроз, будь то хулиганские действия, террористические и кибератаки или распространение коронавирусной инфекции.

Что можно и что нельзя

Для предотвращения всевозможных угроз на государственном уровне принимается система запретов и ограничений, исполнение которых носит общеобязательный характер, а за их нарушение, как правило, предусматривается административная ответственность. К таким запретам и ограничениям добавляются стандарты и правила пользования тем или иным конкретным видом транспорта (метрополитеном, воздушным и др.). Какие-то правила могут выдумываться перевозчиками или же руководством объекта (вокзала, аэропорта и др.) вне утвержденного законодательства и обусловливаться техническими и архитектурными особенностями объекта, на территории которого должен действовать четкий внутриобъектовый режим.

Таким образом, чаша весов между "можно" и "нельзя" для пассажира все больше наклоняется в сторону запретов, несмотря на то, что пребывание и пользование услугами перевозчика для пассажира является платным.

Стоит ли говорить о том, что комфорт пассажиров и качество оказываемых услуг далеко не всегда принимаются во внимание при введении некоторых ограничений.

Опасность транспорта

Проблемам повышения антитеррористической безопасности в большинстве государств уделяется особое внимание, поскольку теракты не только наносят серьезный материальный ущерб, но и становятся известными широкой общественности и оказывают негативное социально-политическое воздействие на население, вызывая напряженность в обществе. Решение этой сложной задачи требует как дополнительных затрат и оснащения транспорта современными техническими средствами, так и адекватных, упреждающих изменений в подходах к технологии и организации перевозочного процесса, оптимизации форм и методов обеспечения безопасности на транспорте[1].

Политика государства в области обеспечения транспортной безопасности должна, с одной стороны, достигать конкретных целей, а с другой – перераспределять и минимизировать ущерб, снижать тяжесть последствий, не только экономических и технологических, но и вообще всех возможных. Задача государства здесь – формировать и проводить политику, направленную на нейтрализацию рисков в транспортной отрасли, в том числе исходящих от международных террористических организаций. Государственная политика в области обеспечения транспортной безопасности посредством перераспределения ресурсов должна способствовать балансу групп интересов в транспортной отрасли[2].

Важно признать, что объекты транспорта относятся к объектам повышенной опасности для пассажиров и лиц, находящихся на этих объектах, будь то провожающие или иные граждане. Связано это в первую очередь с технологическими операциями (движение транспортных средств, функционирование различных технических систем и др.). Дополнительную опасность составляет, конечно же, массовое пребывание граждан на ограниченной архитектурными особенностями территории объектов транспортной инфраструктуры. В условиях текущей санитарно-эпидемиологической обстановки это



Рис. 1. Локализация теракта в Петербургском метрополитене 3 апреля 2017 г.

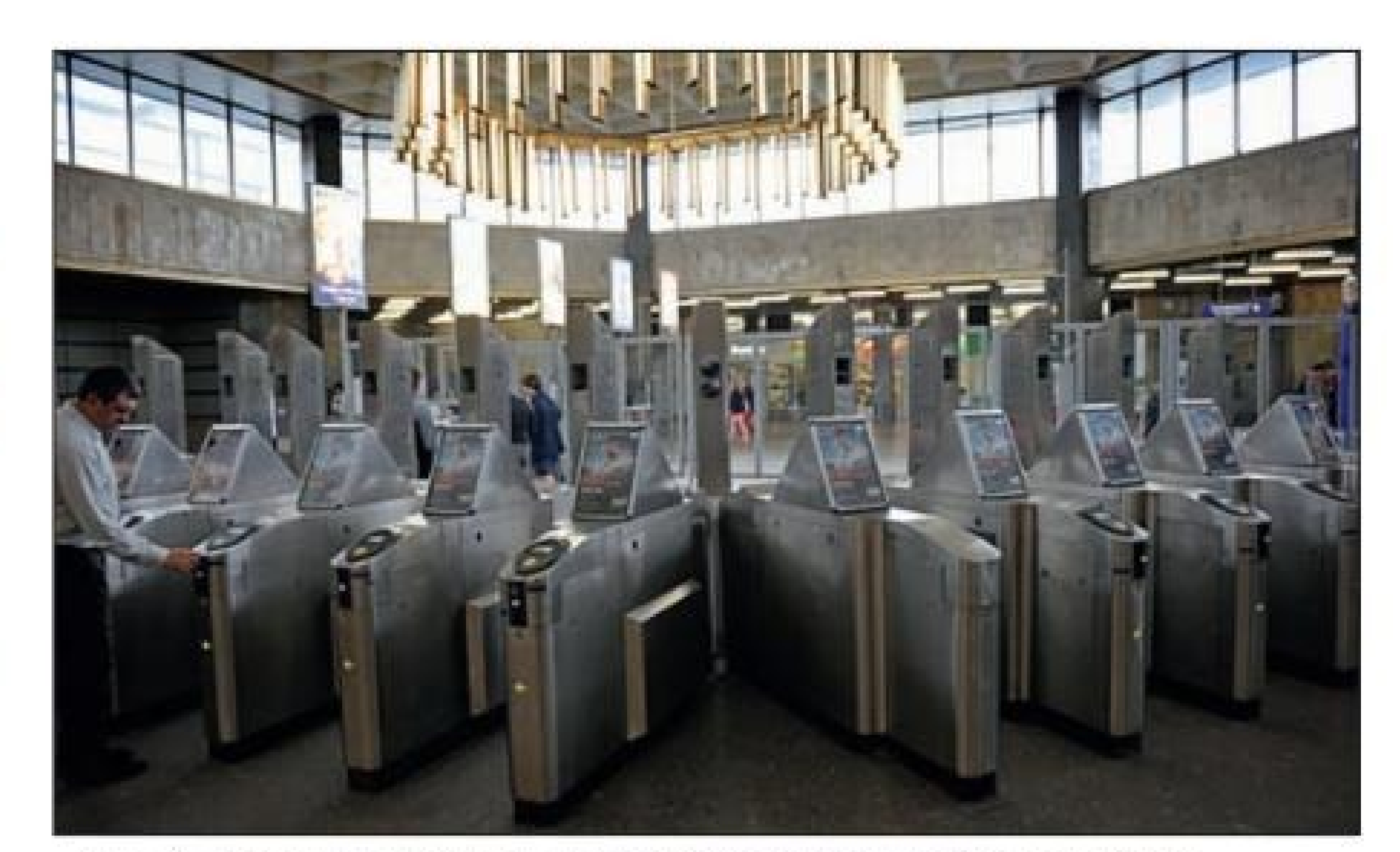


Рис. 2. Оснащение станции Петербургского метрополитена "Ладожская"

[1] *Исаков Д.А. Риск-менеджмент в транспортной инфраструктуре как фактор обеспечения безопасности территорий // Вестник университета (ФГБОУ ВПО "Государственный университет управления"). 2013. № 7. С. 45–49.*
[2] *Тимченко А.В. Институционализация государственной политики обеспечения транспортной безопасности как форма интеграции системы государственной политики // Политическая наука. 2017. Спецвыпуск. С. 124–136.*

приобретает особое значение. Безусловно, угрозы совершения актов незаконного вмешательства (АНВ), в том числе террористических, представляют собой не меньшую, а возможно, и наибольшую опасность для пользователей транспорта. Недаром повышение комплексной безопасности и устойчивости транспортной системы заявлено в качестве приоритетной цели Федеральной целевой программы "Развитие транспортной системы России"[3].

Чем же вызвана такая политика государства и тенденция защиты отдельных объектов инфраструктуры? Конечно, произошедшими террористическими актами на объектах транспорта за последние годы, призванными вызвать общественный резонанс, снизить уровень защищенности граждан, поставить под сомнение принимаемые государством меры и безопасность транспорта. Одним из таких стал теракт в Петербургском метрополитене 3 апреля 2017 г. на перегоне между станциями "Сенная площадь" и "Технологический институт".

По версии Следственного комитета РФ, взрыв осуществил террорист-смертник. В теракте пострадали 103 человека, 16 из них погибли (в их числе исполнитель теракта). В декабре 2019 г. 11 человек, по мнению следствия причастных к организации теракта, были осуждены на сроки от 19 лет лишения свободы до пожизненного заключения.

Вопросы обеспечения транспортной безопасности в последнее время остро обсуждаются в различных государствах всего мира. Трудно переоценить значение мероприятий по укреплению транспортной безопасности для России. Так, надежность транспортного комплекса в процессе обеспечения национальных интересов играет важную роль, которая обусловлена:

1) происходящими в России политическими и социально-экономическими процессами;

2) присущими исключительно ей характеристиками территории;

3) уникальным положением на евразийском континенте[4].

Безопасность транспорта

На момент произошедшего в Петербургском метрополитене теракта (2017 г.) система транспортной безопасности страны, включающая в себя свод законодательства, контрольно-надзорную деятельность, оснащение инженерно-техническими средствами, физическую охрану объектов, профессиональную подготовку и аттестацию и т.д., действовала уже не первый год, а точнее – с 9 февраля 2007 г., то есть с момента издания Федерального закона № 16-ФЗ "О транспортной безопасности". А на воздушном транспорте подобные меры применялись так и вовсе еще в XX веке.

Многое из того, что в аэропортах давно ассоциируется с безопасностью, и сформировало у нас определенные привычки (приезжать на рейс заблаговременно, четко следовать инструкциям работников досмотра и др.), все больше входит в нашу жизнь и на других видах транспорта.

Год от года растущая опасность терроризма и изменчивость его природы свидетельствуют о необходимости периодического пересмотра и уточнения его содержания. Кроме того, данное явление, имея связь с политикой, требует к себе исключительно осторожного отношения. Необходимо учитывать и то, что терроризм – динамичное по своей сути явление и понятие. С момента своего появления он угрожал прежде всего власти и, как любой политический феномен, входил в разряд явлений, связанных с политическим насилием, характеризующимся динамикой своего содержания[5].

Государство и транспортные предприятия тратят огромные средства и усилия во благо безопасности людей. Все тот же теракт 2017 г. в метро привел к необратимым последствиям как для работников транспортной отрасли, так и для пассажиров. Количество сотрудников, задействованных в досмотровых мероприятиях, увеличилось в разы, станции все больше оснащались современными техническими системами безопасности, а досмотр на ряде станций из выборочного стал тотальным (хоть и на короткое время) и максимально приближенным к тому, что мы видим в аэропортах.

Общественный резонанс

Справедливости ради стоит отметить, что описанные меры были выдуманы не самими работниками транспортного предприятия, а продиктованы требованиями законодательства, которые неизменно и в полном объеме соблюдают на воздушном транспорте, но опускают на любом общественном транспорте из-за пассажиропотока.

Одна из ключевых проблем законодательства о ТБ – его универсальность по отношению ко всем видам транспорта (авиационному, морскому и внутреннему водному, автомобильному, железнодорожному и внеуличному) и дорожному хозяйству. Нацеленность закона на формирование единых и прозрачных для всех видов транспорта правил вызывает понимание. Однако им не были учтены нормы юридических институтов, возникших ранее и действовавших на момент его вступления в силу[6].

Ввиду открытости и доступности транспортного предприятия, вездесущности движения транспортных средств, широкого распространения транспортной системы и наличия многих потенциально опасных мест антитеррористические меры безопасности сталкиваются со значительными препятствиями[7].

К чему привели эксперименты с тотальным досмотром на станциях метро? Все к той же социальной и общественной напряженности населения и жалобам граждан в адрес высших должностных лиц города и государства. Получается некий замкнутый круг, в котором и недостаточные, и избыточные меры приводят все к тому же общественному резонансу.

Предупреждение террористических актов на транспорте заключается в проведении эффективных мероприятий по усилению охраны важных объектов (вокзалов, аэропортов, станций метрополитена и других мест транспортной инфраструктуры, так как они чаще всего являются объектами атак террористов). Совершенствование механизма нормативного регулирования требует внедрения самых современных технических средств контроля и защиты, что автоматически подразумевает увеличение ассигнований на подобные цели, разработку и реализацию программ подготовки спецподразделений по обеспечению безопасности на транспорте и объектах транспортной инфраструктуры[8].



Рис. 3. Очередь на входе на станцию "Электросила" Петербургского метрополитена в связи с проведением 100%-го досмотра пассажиров



Рис. 4. Зона досмотра в аэропорту Шереметьево

[3] *Сидоренко А.В., Махина С.Н. Обеспечение транспортной безопасности в современном понимании // Проблемы правоохранительной деятельности. 2018. № 4. С. 70–73.*

[4] *Попова М.А., Переверзева Е.С. Правовое обеспечение транспортной безопасности в России: проблемы и ретроспектива // Сборник Международной заочной научно-практической конференции "Актуальные вопросы современной юридической науки: теория, практика, методика". 2016. С. 213–216.*

[5] *Джинджолия Р.С., Хачидогова М.М. О некоторых вопросах определения терроризма и информационного терроризма // Уголовная юстиция. 2019. № 13. С. 25–28.*

Защищенность или комфорт?

Обеспечение транспортной безопасности в последние годы играет все более заметную роль для государства. Связано это и с некоторыми трагическими событиями, произошедшими в нашей стране, и с развитием технологий в этой области. Однако исполнение некоторых обязательных требований законодательства перевозчиками нередко приводит к дискомфорту со стороны самих пассажиров, для которых этот транспорт функционирует.

Так что же является более важным для государства и для пассажира – безопасность жизни и здоровье или комфорт при пользовании транспортом? Ведь, снижая опасность наступления таких событий, как теракт, и улучшая безопасность перевозок, субъекты транспортной инфраструктуры повышают для себя опасность снижения количества этих самых перевозок в связи с уменьшением пассажиропотока.

Как уже было сказано ранее, система авиационной безопасности и система транспортной безопасности железнодорожного, автомобильного, морского и речного транспорта значительно различаются. Однако с течением времени все меры безопасности на остальных видах транспорта так или иначе приближаются к авиационной безопасности.

Почему вновь вводимые повышенные меры, скажем, на общественном транспорте по-прежнему вызывают у нас негатив? Причин тому можно найти много, но, пожалуй, главная из них – время. Авиационная безопасность как отдельный комплекс мер, предназначенных для защиты гражданской авиации от АНВ, существует несколько десятков лет. Реализация обязательных требований авиаперевозчиками выработала в нас как в пассажирах определенные привычки. Транспортная безопасность иных видов транспорта активно развивается не более десятка лет. Мы все помним, как еще 10 лет назад на различных вокзалах и станциях отсутствовали пункты досмотра, а значит, можно было приехать непосредственно перед отправкой транспорта. Сейчас картина изменилась. Конечно, мы не приезжаем, например, на ж/д вокзал за 1,5 часа, как в аэропорт, но все же минут 5–10 на досмотр мы учитываем. Практически на всех объектах транспорта сейчас имеются технические средства досмотра (металлодетекторы, газоанализаторы и др.).

Еще одной из причин недовольства некоторых людей при прохождении досмотра на различных видах транспорта, кроме воздушного, является его повседневность. Все-таки авиаперелет для подавляющего большинства людей – скорее редкое исключение при пользовании транспортными услугами, чем постоянное правило. Поездки на метро и железнодорожных поездах происходят чаще, а значит, мероприятия по досмотру, включающие в себя обследование человека и его ручной клади техническими средствами, контакт с работником досмотра, тоже случаются намного чаще.



Рис. 5. Зона досмотра Ленинградского вокзала Москвы

Третья, но не последняя причина заключается в том, что в связи с накопленным за десятки лет опытом в области авиационной безопасности большинство аэропортов построены либо реконструированы так, чтобы была возможность осуществлять тщательный (тотальный) досмотр 100% населения, а для самих пассажиров было достаточно места для ожидания. К сожалению, нечто подобное просто невозможно реализовать на некоторых объектах других видов транспорта. К примеру, некоторые вестибюли станций метрополитена в Москве и Санкт-Петербурге оборудованы в высокоэтажных зданиях и провести их реконструкцию в целях расширения площади для досмотра весьма проблематично. Это приводит к выборочному досмотру со стороны перевозчиков и недовольству самих пассажиров работниками досмотра из-за столпотворения в час пик.

Вектор развития

Все вышеперечисленные особенности делают невозможным применение одних и тех же требований в области безопасности на всех видах транспорта, а гонка за обеспечением защиты транспорта со стороны государства и транспортных предприятий грозит привести к росту использования личного транспорта либо попросту к отказу пассажира от идеи воспользоваться общественным транспортом. Данный факт увеличивает опасность ухудшения условий развития транспортной отрасли для самих перевозчиков и субъектов транспортной инфраструктуры.

"В последние годы мы акцентируем внимание на вопросе оптимизации подходов к реализации требований транспортной безопасности в условиях финансовых ограничений и устранения избыточных норм, не оказывающих существенного влияния на состояние антитеррористической защищенности объектов транспорта. Вопрос финансирования мероприятий по реализации законодательства в сфере транспортной безопасности – один из самых важных при обеспечении защищенности транспортного комплекса от актов незаконного вмешательства. Особую актуальность он приобрел в настоящее время, в период сложной экономической ситуации в стране, когда введение секторальных санкций в отношении ключевых элементов нашей экономики негативно отражается на финансовом состоянии хозяйствующих субъектов транспортного комплекса, на которые возложена ответственность за реализацию требований в области обеспечения транспортной безопасности[9]", – именно так прокомментировал заместитель министра транспорта РФ Николай Захряпин курс развития государственной политики в области обеспечения транспортной безопасности в 2017 г.

Будучи министром транспорта РФ, Максим Соколов на итоговой Коллегии Минтранса России 28 марта 2018 г. назвал одной из ключевых целей министерства повышение эффективности и безопасности функционирования транспортного комплекса. Рядом поставлены две взаимосвязанные задачи: продуктивность работы транспорта и обеспечение безопасности его функционирования. Видение безопасности на транспорте как ключевой цели деятельности Минтранса России побуждает задуматься, какими силами, средствами и методами можно добиться устойчивой, гарантированной системы безопасности, при которой транспорт станет продуктивным и привлекательным. Проявление повышенного внимания к проблемам безопасности объясняется тем, что на этапе развития транспортной системы на основе новых технологий увеличивается степень рисков, растут масштабы источников опасности. Если не прилагать новых усилий и не развивать способы, упреждающие угрозы людям и транспортной инфраструктуре, то проблемы обеспечения безопасности будут наращиваться, а транспорт станет терять свою привлекательность, что повлечет за собой причинение огромного вреда нашему Отечеству[10].

Уже более десятка лет государство направляет значительную часть денежных средств на развитие и повышение уровня транспортной безопасности, формирует и совершенствует нормативную базу, изучает и применяет международный опыт. Безусловно, предпосылки для концентрации внимания в данном направлении есть и в мире, и в нашей стране. Проблемы в государственном регулировании данной отрасли существуют, как и во многих других: пробелы и несогласованность норм законодательства, недостаточное количество высококвалифицированных специалистов, низкое качество обслуживания некоторыми специализированными в данной области компаниями и др. Однако хочется верить, что для совершенствования транспортной безопасности в стране просто нужно время. ■

[6] *Семенов С.А. Транспортная безопасность: проблемы становления // Транспорт Российской Федерации. 2018. № 3 (76). С. 19–23.*

[7] *Таова Л.Ю. Терроризм на транспорте как угроза современному обществу // Теория и практика общественного развития. 2014. № 2. С. 156–158.*

[8] *Левин А.О. Предупреждение террористических актов на транспорте // Вестник Московского университета МВД России. 2014. № 5. С. 114–117.*

[9] *Захряпин Н.Ю. Совершенствование государственной политики в области обеспечения транспортной безопасности // Транспорт Российской Федерации. 2017. № 2 (69). С. 3–6.*

[10] *Духно Н.А. Обеспечение безопасности при эксплуатации объектов транспортной инфраструктуры // Транспортное право и безопасность. 2018. № 2 (26). С. 8–19.*



Владимир Балановский
Член бюро комиссии РАН по техногенной безопасности, профессор

Владимир Подъяконов
Научный сотрудник Военного университета МО РФ, к.и.н.

Антон Прокопчук
Начальник центра информационных технологий связи и защиты информации ГУ МВД России по г. Москве

Алексей Авдонов
Генеральный директор "Интерправо Инвест"

Трансформация традиционных нравственных ценностей в виртуальном пространстве

Современное постиндустриальное общество приобретает черты цифрового, в котором главными ценностями становятся информация и знания. В бурно развивающемся киберпространстве происходит трансформация устоявшихся нравственных ценностей, они транслируются безо всякой этической оценки, этот процесс имеет стихийный, хаотичный характер. Наиболее наглядно это можно наблюдать на примере подачи информации цифровыми средствами массовой коммуникации (СМК)

В оценке одной и той же ситуации разными СМК устоявшаяся вековая нравственная ценность может кардинально трансформироваться из добродетели в порок. Такое положение вещей нагнетает напряжение в обществе, приводит к психологическому выгоранию и моральной растерянности, а отсутствие критериев моральной оценки дезориентирует современного человека, создавая внутренние и внешние конфликты.

Безопасность и этика: в чем связь?

В условиях "управляемого хаоса" особенно остро чувствуется, что именно этика определяет моральное развитие социальных институтов и отношений, влияющих на общественную безопасность. Необходим анализ взаимосвязи безопасности и этики, являющихся вроде бы далекими друг от друга категориями: этика исследует нравственность и мораль, порожденные совместным проживанием, нормы, сплачивающие общество, способствующие преодолению индивидуальности и агрессивности, а безопасность – состояние защищенности от нанесения ущерба, способность к сдерживанию или парированию опасных воздействий.

Внутренний терроризм как социокультурный феномен

Формируемое в рамках "управляемого хаоса" пограничное, или, выражаясь техническим языком, "запроектное", агрессивное поведение, воинствующий индивидуализм с его психосоматическими нарушениями становятся основой сложного социокультурного феномена – внутреннего терроризма (ВТ). Он является наиболее острой формой противоборства, возникающей вследствие внутренних противоречий у людей с невысоким интеллектуальным уровнем и пониженной социальной ответственностью, нравственной и моральной беспринципностью на фоне психосоматических нарушений.

Цели

ВТ – это деятельность экстремистски ориентированных политических сил и отдельных лиц по отношению к существующей власти, а также противоборствующих политических сил экстремистской направленности.

В первом случае ВТ направлен на насильственную ликвидацию, изменение общественно-политического строя и государственной политики для достижения политических целей.

Во втором случае цель ВТ – ослабление политических противников, укрепление позиций во внутриполитической борьбе.

Оба вида ВТ связаны с применением любых форм террористической деятельности и направлены на ведение борьбы с существующим строем.

Технологический терроризм

Одно из опасных социальных явлений в форме ВТ – технологический терроризм, инициирующий ЧС и приводящий к дальнейшим каскадным явлениям, а именно:

- актам в форме поджогов, использования радиоактивных, взрывчатых веществ, токсичных химикатов, отравляющих веществ и патогенных биологических агентов;
- акциям против объектов повышенной опасности, разрушение или уничтожение которых ведет к тяжелым последствиям.

Признаки

Для ВТ характерен ряд специфических признаков:

1. Направленность против политической системы и общественной безопасности РФ. Предупреждение и пресечение ВТ – это центральные задачи обеспечения безопасности.

2. Криминализиция. В мире существуют два подхода к уголовно-правовой оценке ВТ – государственные (политические) и преступления общеуголовного характера. Объединение первого и второго подходов применяется в РФ.

Организованная и спонтанная экстремистская деятельность

От международного терроризма ВТ в РФ отличает то, что для него характерно совершение терактов и отдельными лицами, и экстремистскими организациями. В силу ограниченности возможностей террористов-одиночек их деятельность рассчитана на разовые акции и не носит систематического, долговременного характера. В условиях "управляемого хаоса", а соответственно роста активности экстремизма и национализма удельный вес таких терактов возрастает. ВТ возникает как специфическая форма организованной экстремистской деятельности, причем планированию и подготовке терактов отводится значительное место. Для него характерно осуществление акций и спонтанно, без специальной подготовки, в ходе массовых выступлений, так как динамика поведения толпы предполагает инициирование насилия со стороны провокаторов.

Комплекс мер и технических средств для борьбы с ВТ

Борьба с ВТ должна предусматривать формирование более широкого по сравнению с существующим комплекса мероприятий и проектных решений инженерно-технических средств, направленных на обеспечение защиты объектов городской инфраструктуры от угроз террористического характера. Работа ведется на основе анализа механизма зарождения ВТ, его возникновения, формирования, развития и реализации, факторов, которые благоприятствуют осуществлению акций данного вида. К таким факторам при проведении "психологических" операций "управляемого хаоса" с целью деморализации относится использование свойства легкой и быстрой усваиваемости, "просачиваемости" в бессознательное человека, что достигается путем эксплуатации "эффектов" – закономерностей человеческого восприятия.

Особое внимание уделяется индивидуальным особенностям, связанным с психосоматическими нарушениями реализаторов актов ВТ. Необходимо иметь в виду, что внутренний нарушитель – это человек в среднем 28–29 лет, уже имеющий психосоматические нарушения, в лучшем случае в пограничном состоянии, из которого его может вывести любое малозначимое событие – "взмах крыла бабочки". Он нереально воспринимает окружающую действительность в виде виртуальных клипов и без страха способен на "подвиги", как в компьютерной игре. Международный и российский опыт показывает, что таких "шахидов" специально отбирают и целенаправленно воспитывают, поэтому с ними бесполезно бороться или переубеждать на улице. Их толпы, с учетом личности нарушителей, необходимо отправлять в нужном направлении с помощью инженерных средств, используя подмену перехваченных команд инициатора ВТ в мобильной сети.

Новая парадигма обеспечения безопасности должна предусматривать включение новых разработок в области не только технической, но и инженерной защиты как внутриобъектовой, так и прилегающей городской территории. Кроме того, она предполагает разработку комплекса мер и технических средств в виртуальной сфере – в области информационной безопасности в ее гуманитарной составляющей, обеспечиваемой в условиях информационной войны применением специальных технических мероприятий и баз знаний, которые управляются с использованием искусственного интеллекта. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru



Валентин Пашинцев
Ведущий специалист Центра сервисного обслуживания ГУ МВД России по Московской области

Что задерживает внедрение новых технологий в жизнь

В наше время никого не нужно убеждать в преимуществах применения инноваций в самых различных сферах жизни людей и общества в целом, начиная от обеспечения безопасности государства и заканчивая системами умных зданий для создания комфортных условий проживания и трудовой деятельности. Но так ли прост путь новых технологий к потребителю?

После посещения выставок и чтения тематических журналов создается впечатление, что время искусственного интеллекта уже давно наступило. Тут тебе и полная биометрическая СКУД, и камеры, способные распознавать и вести объект по многим параметрам – полу, цвету одежды, наличию маски и т.д. Для автомобилей это номер, марка, цвет кузова и пр. Возможности видеоаналитики просто беспредельны. Казалось бы, вот оно, будущее, пришло! Но здесь возникает вопрос: а много ли где эти современные системы уже используются? На сегодняшний день их активно применяют несколько крупных банков, главные офисы госкорпораций, стратегические объекты. И всё!

В этой статье я попробую разобраться, что именно задерживает поступь технического прогресса.

Каковы причины медленного внедрения новых технологий?

Почему инновации внедряются не так быстро, как следовало бы? Причин тому существует множество, как общего характера, так и частного, зависящего от конкретной сферы, организации, людей. Ниже проанализирую те, которые считаю основными.

Консервативное мышление людей

Еще Шекспир говорил, что человеку более свойственно "мириться со знакомым злом, чем бегством к незнакомому стремиться". Применение инноваций всегда связано с дополнительными хлопотами: это монтаж нового оборудования, изучение его работы, обучение персонала. Зачем же такая головная боль, когда и так все более-менее работает?

Цена вопроса

Поскольку вендор, стремясь "снять сливки", завышает цену на последние разработки, то и приобретение, и инсталляция новой техники требуют серьезных финансовых вложений. Представьте себе такую ситуацию: начальник службы безопасности приходит к финдиректору предприятия и говорит, что "нам надо приобрести установку с искусственным интеллектом, которая заменит четырех охранников", и называет сумму. На что тот отвечает: "Да я за эти деньги им десять лет могу зарплату платить и спрошу с них, если чего. А с этой машины какой спрос?"

Недоверие к заявленным производителем характеристикам товара

Речь не идет о преднамеренном обмане, хотя такое тоже случается на рынке. Просто вендор иногда поставляет аппаратуру, которая не может корректно работать в нужных заказчику условиях. Например, то, что хорошо работает в офисе на 50 человек, может начать глючить при нагрузке в 500 или же не выдержать условий окружающей среды. В подобных случаях вина не только производителя. Проблемы здесь могут создаваться из-за ошибок менеджера по продажам, не сумевшего правильно подобрать оборудование, либо самого заказчика, неправильно составившего техзадание: "мы так хотим, чтоб подешевле да получше".

Вендоры и крупные дилеры должны быть кровно заинтересованы в повышении уровня подготовки инсталляторов, поскольку это прямым образом влияет на оценку потребителем поставляемого оборудования

Недостаточная квалификация инсталляторов

Как известно, если система неправильно смонтирована и установлена, она никогда не будет работать как положено. Помню, 10 лет назад, когда пошли первые 16-камерные IP-видеосистемы, по прошествии некоторого времени после установки они переставали работать (отключались камеры, зависали системы и пр.). Уже стоял вопрос о разрыве контракта и замене IP-систем на аналог. Хорошо, что в техподдержке поставщика нашелся инженер, который объяснил, что такое битрейт, пропускная способность сети, для чего нужны разные потоки камер и многое другое. Мы часами общались по телефону, настраивая системы. И о чудо! Системы нормально заработали и работают до сих пор. Это я все к тому, что качество работы оборудования из области безопасности, а соответственно и репутация вендора в глазах конечного пользователя во многом зависит от установщика. Ведь ни один инсталлятор не скажет заказчику, что "система не оправдала ожиданий, потому что это я некомпетентен". Скорее всего, он заявит, что это оборудование плохое. А представителю производителя потом бегать, доказывая, что это не так.

Распространенные заблуждения (на примере радиоканальных систем ОПС)

Для иллюстрации вышесказанного приведу результаты исследования по радиоканальным системам ОПС, проведенного в прошлом году. Я изложу основные заблуждения опрошенных, после чего прокомментирую их.

Высокая стоимость оборудования

Да, стоимость устройств радиотехнических систем выше проводных, но если вычесть цену несгораемого провода, кабельных каналов, подвесов, лотков и т.д., а также стоимость монтажа всего перечисленного, то разница в стоимости существенно нивелируется. А если количество устройств в системе превышает 100 штук, то затраты на обе системы сравниваются, а далее радиосистема становится дешевле проводной.

Проблемы надежности и загруженности эфира

Малая надежность работы радиосистем по сравнению с проводными, перегруженность эфира при использования большого количества устройств. Часто говорят, что плохая радиосвязь возникает из-за эфирных помех. Да, такое бывает. Но каждая помеха характеризуется конкретными параметрами: частотой, интенсивностью и амплитудой. Что мешает перед установкой системы проверить эфир анализатором поля и выбрать наименее зашумленный диапазон? Теперь о трафике: дело в том, что устройства не общаются между собой голосом типа "Контроллер шесть, я датчик два, как слышите меня? Прием!". Взаимодействие между ними происходит сериями импульсов длиной менее миллисекунды. К тому же способность системы самой находить оптимальный путь для сообщений существенно повышает надежность передачи данных.

Срок службы батарей

При обсуждении достоинств и недостатков радиоканальных систем практически всегда упоминается большая стоимость их эксплуатации в связи с частой заменой элементов питания. Во-первых, качество и долговечность батарей все время улучшается. Заявленный производителем срок службы современных батарей составляет 10 лет. А во-вторых, повышенный разряд элементов питания возникает из-за неправильной установки устройств. Вы, наверное, не раз замечали, что ваш смартфон, попадая в глухую зону, начинает быстро разряжаться. То же самое происходит и с батареей датчика. Если связь плохая, то датчик будет постоянно находиться в режиме поиска, то есть подавать сигналы для радиорасширителя, пока

не получит ответ. Естественно, срок службы батареи значительно сократится. Но в современных системах качество соединений постоянно контролируется самой системой, позволяя вовремя принимать необходимые меры. Еще не надо забывать о том, что время работы батарей сильно сокращается при использовании оборудования в помещениях с отрицательными температурами.

Возможность влиять на работу радиосистемы извне

В современных системах применяется динамическое 128-битное шифрование, исключающее возможность как-то влиять на работу системы. Разве что можно заглушить систему, но для этого надо иметь глушитель немалой мощности. Например, армейская "Пелена" гарантированно подавляет радиосигнал в радиусе 100 м. Для защиты колонны техники этого достаточно, а для нанесения вреда объекту – вряд ли.

Комментарии к результатам опроса

Необходимо отметить, что в опросе принимали не последние на своих предприятиях специалисты. А что же тогда хотеть от простого монтажника?

В связи с этим можно сделать вывод, что вендоры и крупные дилеры должны быть кровно заинтересованы в повышении уровня подготовки инсталляторов, поскольку это прямым образом влияет на оценку потребителем поставляемого оборудования. Да, многие вендоры производят обучение желающих, но это порой стоит немалых денег. Господа! Это не то, на чем нужно много зарабатывать. Хорошая квалификация инсталлятора – это гарантия надежной работы вашей техники. К тому же общение с эксплуатационниками позволит вам получить сведения о работе оборудования в течение всего срока его жизни, что позволит выявить слабые места и повысить надежность техники. Обучение можно проводить и удаленно, что обойдется много дешевле очного обучения.

Каждый прошедший курс обучения после экзамена должен получить сертификат. Чтобы слушатели ответственно относились к занятиям, третью и последующую пересдачу теста следует сделать платной. Надо также ввести правило, что фирма гарантирует работу техники, только если оборудование устанавливается сертифицированным специалистом.

Следует также отметить, что для увеличения продаж оборудования необходимо работать со всеми группами потенциальных клиентов.

Потребителей систем безопасности можно разделить на несколько групп:

1. Государство:
- стратегические объекты;
- муниципальные предприятия.

2. Коммерция:
- концерны;
- средний бизнес.

3. Малый потребитель:
- мелкий бизнес;
- частный сектор.

Соответственно, к каждой группе заказчиков должен быть свой подход.

Специфика заказчиков и некоторые методы работы с ними

В этой статье я изложил основные причины медленного роста рынка продаж оборудования безопасности, особенно инновационной техники. Но увеличить продажи можно, вдумчиво работая с потребителем, используя соответствующие приемы маркетинга.

В госпредприятиях, как правило, работа ведется с конкретными людьми, принимающими решения или дающими обоснованные рекомендации. Хотя система тендеров и не позволяет бюджетному предприятию решать вопрос с конкретной фирмой, но выход из этой ситуации обычно находят.

В коммерции, как правило, деньги считают, поэтому здесь во главе угла стоят соотношение "цена – качество" и экономическая эффективность вложения. Притом если крупный бизнес, у которого расход на новое оборудование безопасности составляет незначительную часть от оборота, может позволить себе технику премиум-диапазона, то для среднего бизнеса стоимость и эффективность являются приоритетными показателями при закупке.

Основными способами привлечь внимание к своей продукции представителей вышеперечисленных групп заказчиков являются:
- информирование о новых разработках вендоров – выставки, вебинары, презентации;
- обоснованные расчеты, показывающие экономическую эффективность внедрения нового оборудования;
- разумная ценовая политика;
- пробная поставка части систем, позволяющая заказчику наглядно убедиться в надежности и удобстве новой техники.

Что касается мелкого бизнеса и частного заказчика, то тут требуется совсем другой подход, основанный на приемах маркетинга. Но компаниям, которым удастся создать спрос на системы безопасности в этом сегменте рынка, гарантирован резкий взлет продаж своей продукции. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

МНЕНИЕ ЭКСПЕРТА

Еще раз о безопасности объектов ТЭК



Олег Филиппов
Консультант Института комплексной безопасности Самарского ГТУ

В журнале "Системы безопасности" № 1/2021 опубликована статья "Защита объектов ТЭК: нужны перемены!". Однозначно согласен с этим утверждением, перемены нужны. Как справедливо заявляют авторы, "в целом система физической защиты объекта ТЭК законодательно определена". Нормативные правовые акты, разработанные уполномоченными на это органами по вопросу организации безопасности объектов ТЭК, вполне позволяют выполнить все задачи, определенные в Федеральном законе № 256 "О безопасности объектов топливно-энергетического комплекса".

Главным "тормозом" решения задач категорирования объектов ТЭК и анализа уязвимости объекта в целом считаю навязывание предшествующими рабочими группами методических рекомендаций по анализу уязвимости производственно-технологического процесса и выявлению критических элементов объекта, оценке социально-экономических последствий совершения на объекте террористического акта и антитеррористической защищенности объекта при категорировании, составлению (актуализации) паспорта безопасности объекта топливно-энергетического комплекса (октябрь 2012 г.) в качестве нормативного акта. Даже неподготовленному специалисту при изучении будет очевидным несоответствие их содержания постановлению Правительства РФ от 5 мая 2012 г. № 459 "Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования" и постановлению Правительства РФ от 5 мая 2012 г. № 458 "Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса".

Совершенствовать методическое обеспечение выполнения задач безопасности и антитеррористической защищенности для объектов ТЭК, на мой взгляд, невозможно без участия специализированных организаций, накопивших большой опыт их практического решения. К сожалению, площадки для обсуждения вопросов безопасности объектов ТЭК нет, а следовательно и не будет положительного результата.

Все эти проблемы можно объединить в одну главную – низкий уровень ответственности и подготовки специалистов органов управления системой физической защиты субъекта ТЭК, Росгвардии как контрольно-надзорного органа, а также представителей других министерств и ведомств, участвующих в решении задач безопасности объектов ТЭК.

Решение этих задач в настоящее время зависит только от субъекта ТЭК. Руководитель несет ответственность за безопасность и антитеррористическую защищенность своего объекта, значит, его полномочия предполагают правовые возможности достичь установленной цели. ■



Искусственный интеллект как инструмент в автоматизации зданий

В статье "Новые аспекты автоматизации зданий", опубликованной в журнале "Системы безопасности" № 1/2021, упоминалось использование ИИ в системах автоматизации зданий. Появившийся в начале 2000-х гг. термин "интеллектуальное здание" был весьма популярным, однако реально отражал лишь уровень исполнения систем автоматизации здания, не имея прямого отношения к его "интеллектуальности". Сегодня уже можно говорить об оптимизации функционирования инженерных систем здания на базе автономного анализа данных, которая достигается за счет использования ИИ

Владимир Максименко
Эксперт сектора обучения и информационной поддержки НВП "Болид"

В современных системах автоматизации зданий изменение положения солнца в течение дня может быть учтено при управлении освещением, шторами, а также отоплением и кондиционированием. Работа систем вентиляции может быть основана не только на сигналах датчиков присутствия и CO_2, но и на графиках занятости конкретных помещений, уборки и санобработки, особенно актуальных в последнее время. Более того, могут быть использованы прогнозы, сделанные на основе накопленных данных о профилях работы инженерного оборудования в предшествующий период. Такое превентивное управление зданием может применяться практически для любых систем и обеспечивает снижение потребления энергии, сокращение эксплуатационных расходов, повышение эффективности использования помещений и т.д.

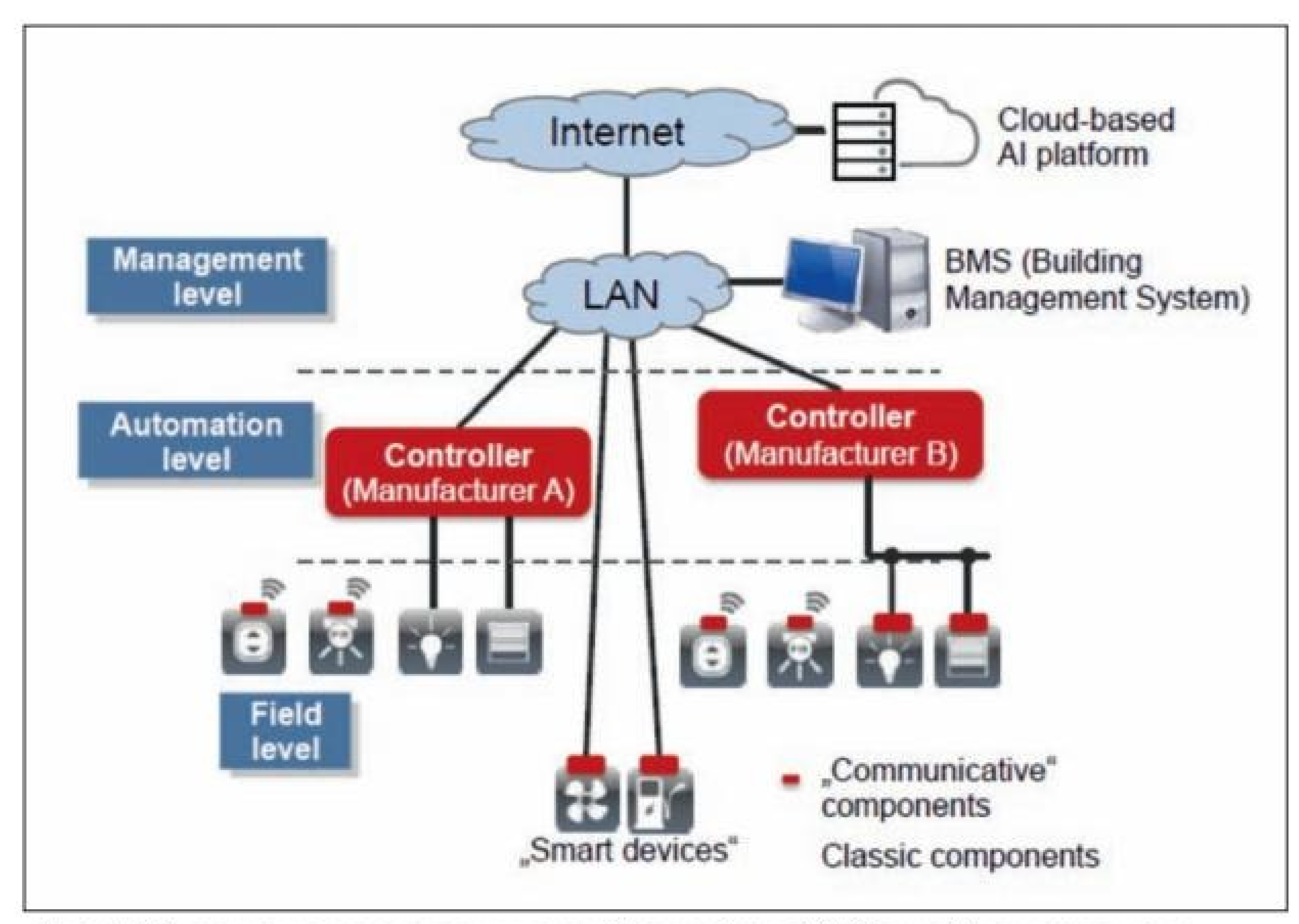


Рис. 1. Объединение автоматизации зданий с платформой (облачной) искусственного интеллекта

Переход от интеллектуального к обучаемому зданию

Активное внедрение ИТ в системы автоматизации зданий в последнее время повлекло за собой новые возможности в части использования современных средств программирования и языков, удобной визуализации для разных групп пользователей и открыло путь к быстрой обработке больших объемов данных от инженерного оборудования, являющейся, по сути, элементом ИИ. Эти прогнозные методы управления инженерным оборудованием зданий

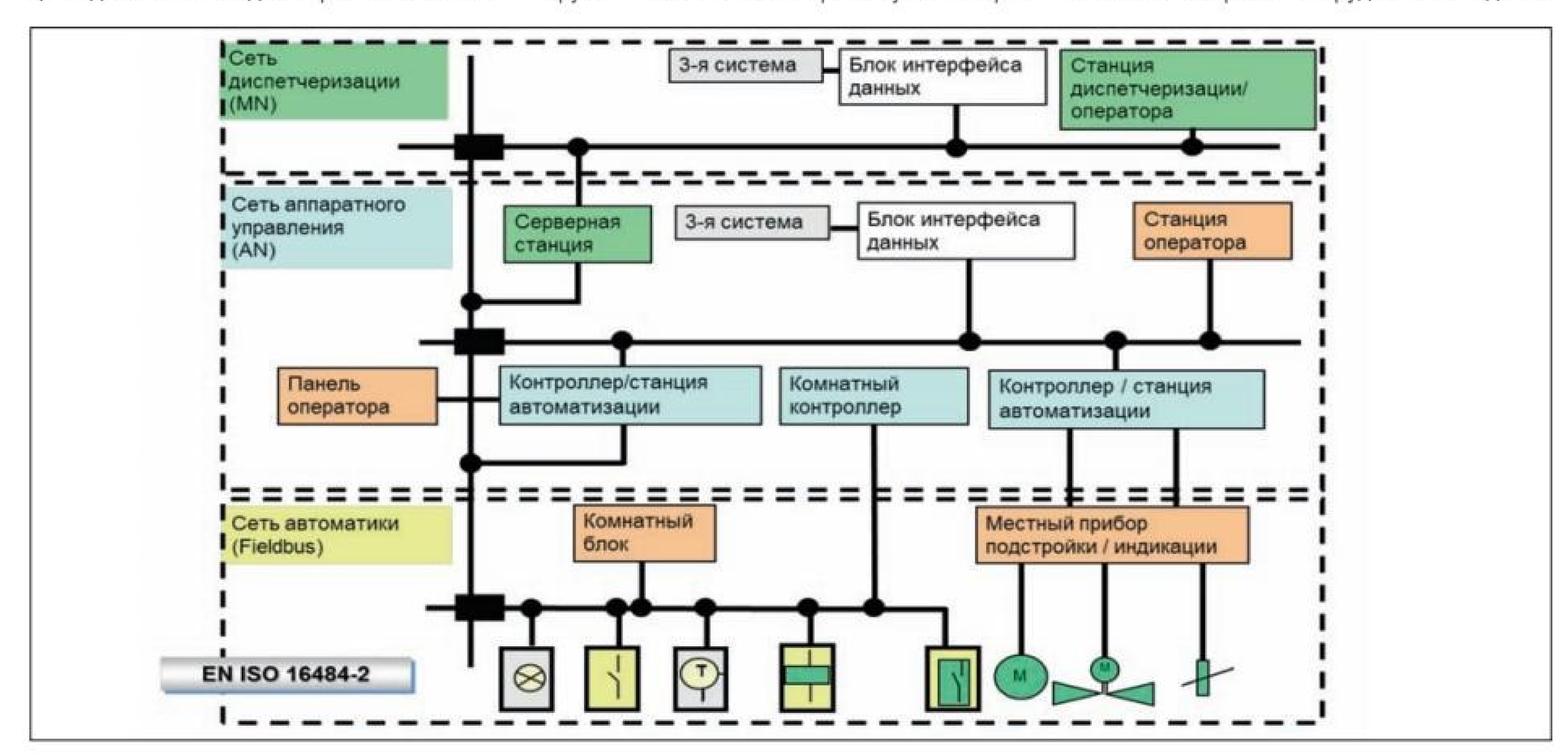


Рис. 2. Структура системы автоматизации здания

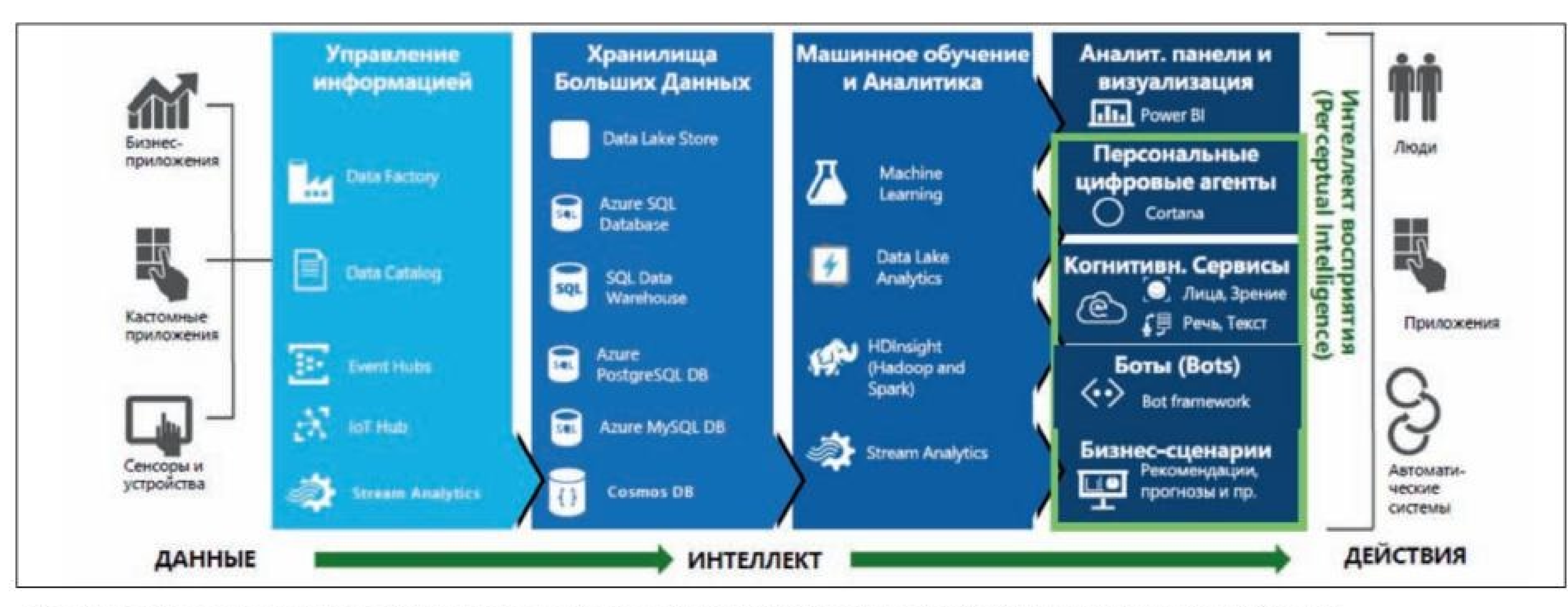


Рис. 3. Платформа интеллектуальных сервисов работы с данными Azure (искусственный интеллект и машинное обучение)

обеспечивают переход от интеллектуального здания к обучаемому или когнитивному. Упомянутый переход происходит при наличии ряда необходимых условий, к которым относятся, по крайней мере, соответствующие строительная инфраструктура, архитектура системы и приложения. Наличие этих условий позволяет обеспечить переход к системному обучению, формирующему технологии ИИ.

Строительная инфраструктура

Строительная инфраструктура, использующая ИИ, ведет не только сбор данных от большого количества датчиков, но и их хранение для последующей обработки и анализа. При этом чем больше полнота получаемых данных, тем более качественным будет реакция ИИ. Поскольку устанавливаемые для решения этой задачи проводные датчики также требуют обслуживания, представляет большой интерес использование беспроводных датчиков, не требующих обслуживания.

Архитектура системы

Архитектура системы – это платформа, поддерживающая процессы обучения. Она может быть как облачной, так и серверной. Серверные обладают большей вычислительной мощностью, а облачные – более широким функционалом. Необходимо отметить, что платформа ИИ строится на инфраструктуре системы автоматического управления зданием, которая управляет инженерным оборудованием здания и обеспечивает контроль систем автоматизации помещений. В этом смысле интересно отметить, что предлагаемая зарубежными специалистами[1] структура объединения автоматизации зданий с платформой (облачной) искусственного интеллекта во многом совпадает со структурой системы автоматизации здания, приведенной в стандарте ISO 16 4842. Обе структуры имеют три уровня – полевой, аппаратного управления и диспетчеризации (менеджмента), только при объединении с облачной платформой активнее используются облачные технологии, и на уровне менеджмента появляется облачная платформа ИИ, обеспечивающая новый качественный уровень решения, на котором возможна реализация обучаемого здания.

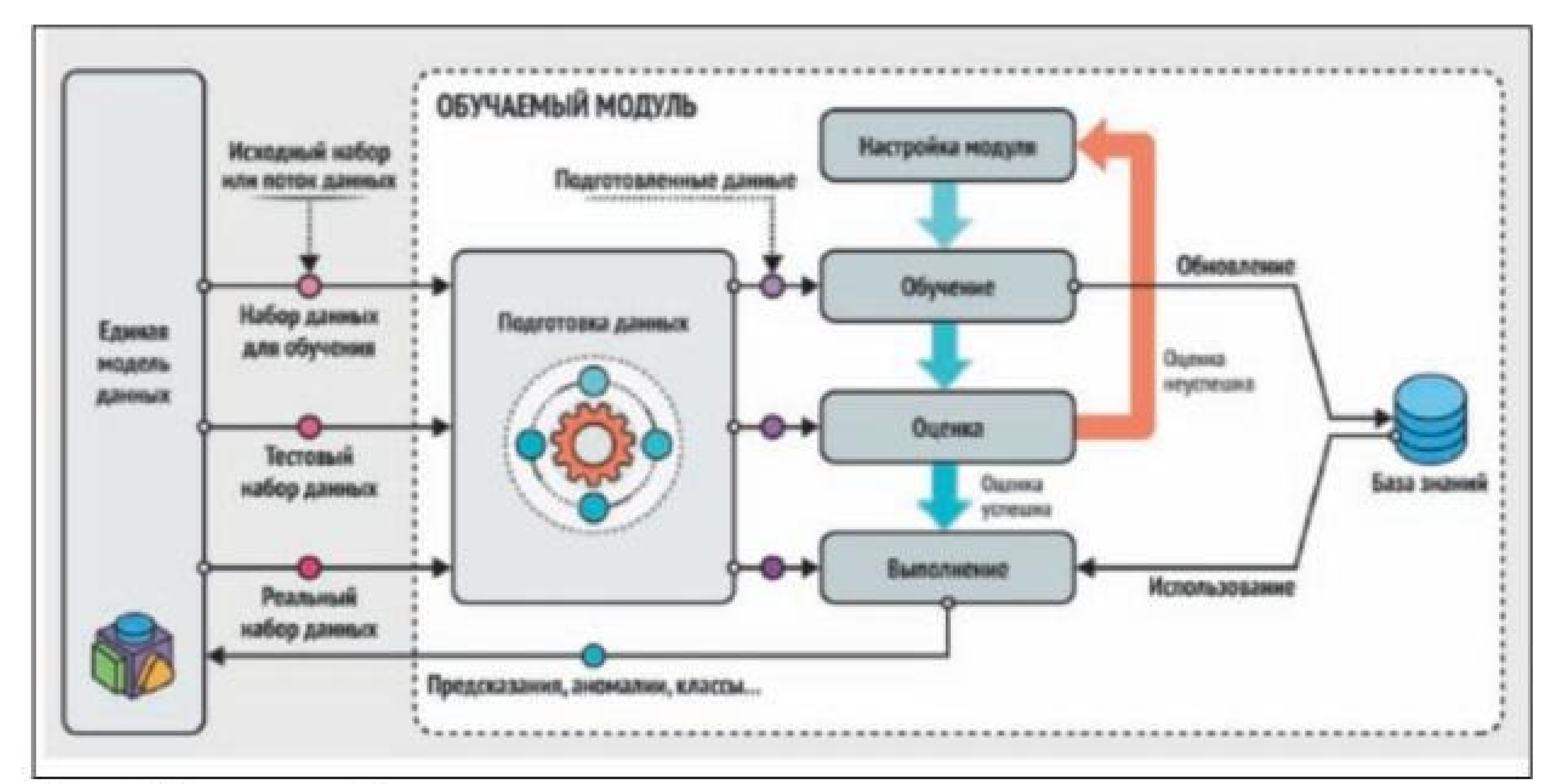


Рис. 4. Машинное обучение

Приложения

Приложения на основе ИИ можно разделить на условные категории, такие как:

- оптимизированное управление оборудованием объекта, инфраструктурой и площадями;
- управление нагрузками;
- превентивное обслуживание;
- повышение эффективности использования персонала;
- предоставление платных услуг;
- повышение эффективности использования датчиков.

В качестве примера платформы интеллектуальных сервисов можно привести платформу Azure компании Microsoft[3].

Как видно из рис. 3, платформа в своем блоке интеллекта содержит модуль машинного обучения и аналитики, обеспечивающий анализ поступающей информации и формирование на основе актуальной и ранее полученной информации управляющих воздействий.

Алгоритм машинного обучения более подробно приводился на онлайн-саммите "Умные дома и здания в России"[4]. Он применяется для предсказания значения, определения аномалий и классификации наборов данных.

Цель определяет средства

Подводя итог теме использования ИИ в качестве инструмента автоматизации зданий, следует отметить, что требования и задачи заказчика определяют архитектуру IoT интеллектуального здания и соответствующие устройства, а не наоборот. В свою очередь, применение технологий ИИ позволяет использовать широкий спектр приложений в области автоматизации зданий. Практические результаты, планируемые как эффект от реализации решений на основе ИИ, необходимо точно обозначить на начальном этапе работы с проектом, поскольку "это играет определяющую роль в выборе процесса обучения и его моделирования, а также в выборе платформы ИИ и типа, количества и расположения датчиков сбора энергии, необходимых для ввода данных"[1]. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

[1] *Artificial Intelligence in The Field of Building Automation. Professor Michael Krödel, CEO, Institute of Building Technology, Ottobrunn, Germany and Professor for Building Automation and Technology, University of Applied Sciences at Rosenheim and Graham Martin Chairman & CEO, EnOcean Alliance.*
[2] *Системы автоматизации и управления зданиями. АВОК СТАНДАРТ-5-2004. Часть 2. Основные положения. Аппаратные средства.*
[3] *Онлайн-саммит "Умные дома и здания в России". "Умные города и умные здания". Данилин А., компания Microsoft. Доклад.*
[4] *Онлайн-саммит "Умные дома и здания в России". Платформа Интернета вещей на Edge. Коржебин А., Tibbo systems. Доклад.*

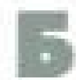
А

АДЖАКС СИСТЕМС, ООО
119435, Москва, пер. Б. Саввинский, 12, стр. 8, этаж 3, пом. I, комн. 53, 54
Тел.: 8 (800) 500-3267
E-mail: support@ajax.systems
https://ajax.systems/ru/
См. СПЕЦПРОЕКТ Ритейл на стр. 39

АРГУС-СПЕКТР, ООО
197342, Санкт-Петербург,
ул. Сердобольская, 65, лит. А
Тел.: +7 (812) 703-7500
E-mail: mail@argus-spectr.ru
www.argus-spectr.ru, стрелец.рф
См. ст. "Защита от ложных срабатываний в беспроводной системе пожарной сигнализации "СТРЕЛЕЦ-ПРО" на стр. 66, 67

АРМО-Системы, ООО
125167, Москва, Ленинградский пр-т, 37А, корп.14, БЦ "АРКУС-II"
Тел.: 8 (800) 700-3343,
+7 (495) 787-3342
E-mail: armosystems@armo.ru
http://armosystems.ru
См. СПЕЦПРОЕКТ Ритейл на стр. 37

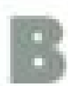
АСТРОН, ОКБ, АО
140080, г. Лыткарино Московской обл., ул. Парковая, 1
Тел.: +7 (495) 215-1382
E-mail: info@astrohn.ru
www.astrohn.com, www.astrohn.ru
См. СПЕЦПРОЕКТ COVID-Tech. Оборудование для термометрии на стр. 11



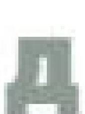
БЕВАРД, НПП, ООО
117198, Москва,
ул. Миклухо-Маклая, влад. 8, стр. 3
Тел.: +7 (495) 505-6341,
+7 (391) 278-9200
E-mail: moscow@beward.ru
www.beward.ru
См. клапан на 1-й обл.
См. СПЕЦПРОЕКТ Ритейл на стр. 38
См. стр. 85

БИК-ИНФОРМ, ООО
190020, Санкт-Петербург,
ул. Бумажная, 9, корп. 1
Тел.: +7 (812) 447-9555
Факс: +7 (812) 447-9556
E-mail: bic@bic-inform.ru
www.bic-inform.ru
См. стр. 87

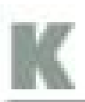
БОЛИД, НВП, ЗАО
141070, г. Королев Московской обл.,
ул. Пионерская, 4
Тел.: +7 (495) 775-7155
E-mail: info@bolid.ru
www.bolid.ru
См. ст. "Распознавание лиц – новое качество ИСО "Орион"!" на стр. 58, 59
См. СПЕЦПРОЕКТ Охранный мониторинг. ПО для охранных предприятий на стр. 103



Витэк-Автоматика, ООО
198035, Санкт-Петербург,
наб. реки Фонтанки, 170
Тел.: +7 (812) 575-4591
E-mail: info@vitec.ru
www.vitec.ru
www.visionmachines.ru
См. стр. 97



дормакаба Евразия, ООО
117036, Москва,
ул. Дмитрия Ульянова, 7а
Тел.: 8 (800) 250-1576,
+7 (495) 966-2050
E-mail: info.ru@dormakaba.com
www.dormakaba.com/ru-ru
См. СПЕЦПРОЕКТ Ритейл на стр. 39
См. стр. 69



Кибер Айконтрол, ООО
197101, Санкт-Петербург,
ул. Мира, 3, офис 327
Тел.: 8 (800) 301-3970
E-mail: v.ogait@cvc.ai
www.cvc.ai
См. СПЕЦПРОЕКТ Видеонаблюдение в ритейле на стр. 83

Р

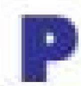
РекФэйсис, ООО
119334, Москва,
5-й Донской пр-д, 21Б, стр. 10
Тел.: +7 (495) 268-0893
E-mail: sales@recfaces.ru
https://recfaces.com
См. СПЕЦПРОЕКТ Ритейл на стр. 37

С

"СОКРАТ" Охранное бюро, ООО
664007, Иркутск,
пер. Волконского, 2
Тел.: +7 (3952) 640-663,
8 (800) 3000-66-70
E-mail: sokrat@sokrat.ru
www.sokrat.ru
См. СПЕЦПРОЕКТ Охранный мониторинг. ПО для охранных предприятий на стр. 103



AXIS COMMUNICATIONS, ООО
125284, Москва,
Ленинградский пр-т, 31А, стр. 1, этаж 16
Тел.: +7 (495) 940-6682
www.axis.com
См. ст. "Высокоскоростная PTZ-камера AXIS Q6135-LE для съемки в темноте на большие расстояния" на стр. 7



PERCo
194021, Санкт-Петербург,
ул. Политехническая, 4,
корп. 2, стр. 1
Тел.: 8 (800) 333-5253,
+7 (812) 247-0457
E-mail: market@perco.ru
www.perco.ru
См. СПЕЦПРОЕКТ COVID-Tech. Оборудование для термометрии на стр. 11



СИСТЕМЫ БЕЗОПАСНОСТИ
SECURITY AND SAFETY

Эффективное комьюнити профессионалов, организующее общение специалистов через печатное издание, интернет-портал и онлайн-мероприятия.

Журнал "Системы безопасности"

Издается компанией "Гротек" с 1995 года.
Тираж 25 000 экземпляров. Периодичность выхода: один раз в два месяца. Объем 120–144 страницы.
Распространение: платная подписка на печатную и электронную версии издания, бесплатная квалифицированная подписка, адресная доставка, распространение на отраслевых выставках.

Сайт Secuteck.Ru

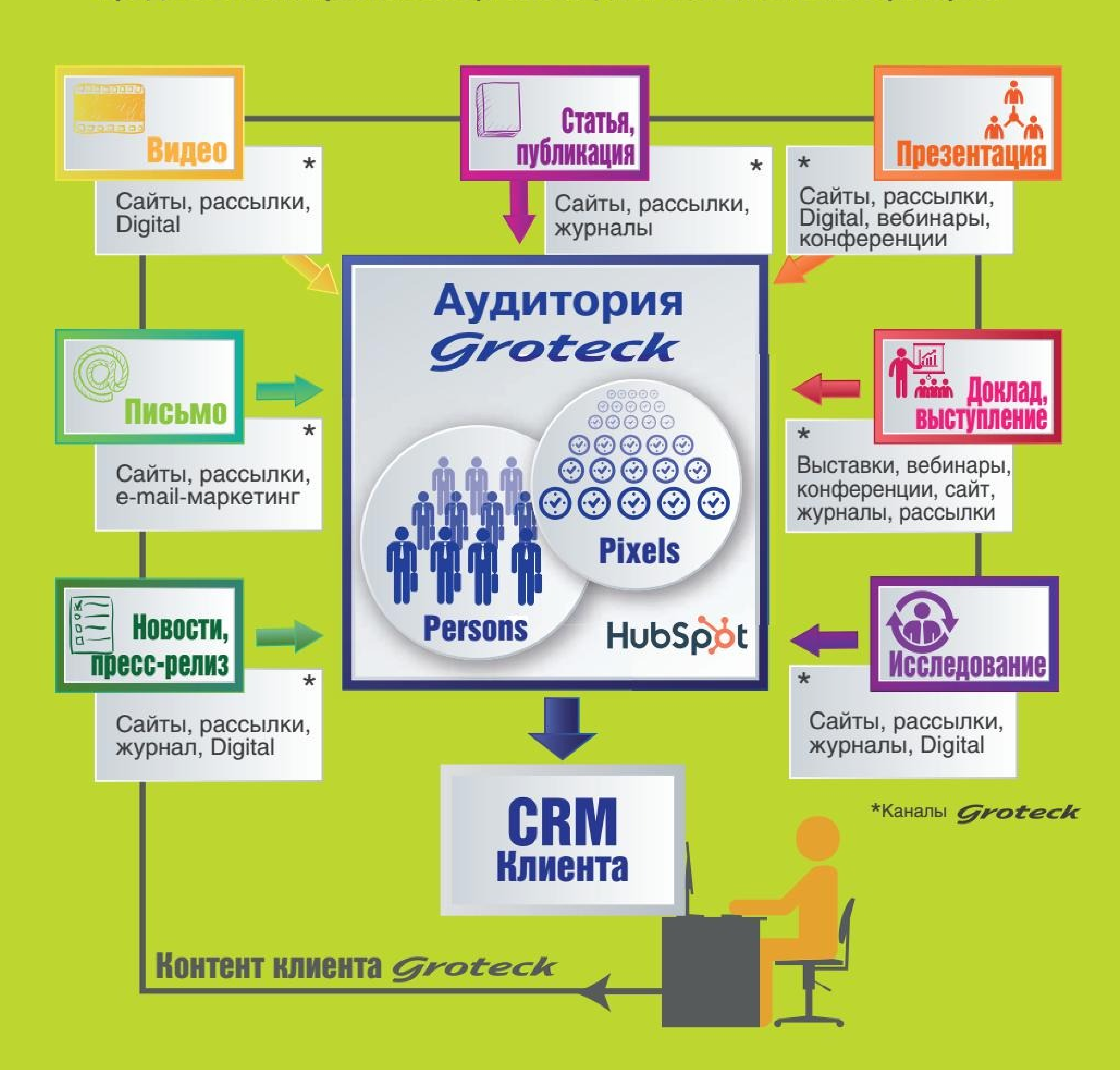
Интернет-ресурс проекта "Системы безопасности", на котором ежедневно публикуются новости отрасли, статьи по видеонаблюдению и видеоаналитике, системам контроля доступа и биометрии, охранно-пожарной сигнализации и пожарной безопасности, об искусственном интеллекте и беспилотниках, о цифровизации и умном городе и т.д.
В 2020 году на сайте было опубликовано более 1500 новостей, более 250 статей, более 70 обзоров оборудования, рынков и результатов исследований. Годовая аудитория сайта – более 310 000 уникальных посетителей, которые просматривают 800 000 страниц. Подписку Secuteck Weekly еженедельно получают более 1500 человек.

Мероприятия Secuteck ADAPT

Площадка для онлайн-мероприятий, на которой в 2020 году прошло 75 конференций, встреч с заказчиками, вебинаров и круглых столов. Мероприятия посещают специалисты разных сфер безопасности со всей страны, спикерами выступают лучшие эксперты отрасли, аудитория конференций составляет от 150 до 500 человек.

ЛИДОГЕНЕРАЦИЯ В ИНТЕРЕСАХ КЛИЕНТА Groteck

Аудитория компании "Гротек" и проекта "Системы безопасности" – это руководители, принимающие решения о закупках, технические специалисты всех ключевых отраслей российской экономики, представители проектных организаций и системных интеграторов.



ПРЕИМУЩЕСТВО "ГРОТЕК" – ВЫСОКОЭФФЕКТИВНЫЕ КАНАЛЫ КОММУНИКАЦИИ И ДОСТОВЕРНАЯ, ЛОЯЛЬНАЯ, СЕГМЕНТИРОВАННАЯ АУДИТОРИЯ